IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

BERNARDINE GRIFFITH; et al., individually and on behalf of all similarly situated,	§	
Plaintiffs,	§	
v.	§	**Case No. 5:23-cv-00964**
TIKTOK, INC., a corporation BYTEDANCE, INC., a corporation	§	
Defendant.	§	

EXPERT REPORT OF BRUCE SCHNEIER

SEPTEMBER 20, 2024

I. Introduction 3

II. Case Background 3

III. Assignment and Methodology 4

IV. Expertise 5

V. Summary of Opinions 7

VI. Individuals Have a Reasonable Expectation of Privacy on the Internet 8

1. Privacy 8
1.1. "Private" and "Privacy" Have Specific Meanings and Implications 8
1.2. Privacy Is a Basic Human Need 9
1.3. Privacy Is Crucial for Political Liberty and Justice 10

2. Data Privacy 11
2.1. People Have Been Denied the Ability to Make Meaningful Internet Privacy Choices 11
2.2. Privacy Has Become More Important with Widespread Corporate Surveillance 12
2.3. The EU, As Well as Several US States, Has Passed Comprehensive Data Privacy Laws 14

3. Personal Online Data 16
3.1. Browsing Information Can Be Highly Revealing 16
3.2. Personal Data Generates Billions in Corporate Revenue 18

4. Individual Attitudes Towards Privacy 23
4.1. People's Privacy Intuition Is Suited to Face-To-Face Interactions 23

VII. Individuals Have a Reason to Avoid Surveillance by TikTok 24

5. TikTok has a Surveillance-Dependent Business Model 24
5.1. The TikTok Pixel and Even s API Co tribute to a Sign icant Revenue Source for TikTok 24
5.2. Non-TikTok User Data Collected by the TikTok Pixe and Events API [redacted] 24

6. The Data Collected by the TikTok Pixel and Events API Causes Significant Privacy Risk 26
6.1. It is Practically Impossible to Avoid the TikTok Pixel or Events API while Using the Internet 26
6.2. TikTok Collects Sensitive And/Or Identifying Personal Online Data From Non-TikTok Users 28
6.3. "Hashing" of Collected Data Does Very Little to Mitigate the Privacy Risk 29
6.4. The Volume of Data Collected by TikTok Is Tremendous 29
6.5. TikTok Fails to Provide Adequate Notice or Obtain Non-TikTok Users' Consent 30

7. TikTok's Affiliation with the Chinese Government and History of US-Based Privacy Violations Heightens the Risk 31
7.1. TikTok Has a History of Privacy Violations 31
7.2. The Chinese Government Routinely Engages in Online Espionage Against the US and Its Allies 36
7.4 TikTok Is Legally Mandated to Provide Data to the Chinese Government If Ordered to Do So 48
7.5 TikTok Has Historically Stored US Data Overseas, and Sent Some US Data to Its Data Center in Singapore 49
7.6 Non-TikTok Users Have Reasons to Deliberately Attempt to Avoid Surveillance by TikTok 49

VIII. Conclusion 54

I. Introduction

1. The rise of the Internet and surveillance business models has increased threats to privacy, making it more important than ever for users of the Internet ("users") to have a refuge from pervasive tracking. The volume and scope of data people generate while using the Internet reveals information about individual users, which is highly valuable to commercial actors. Accordingly, effective protection of privacy requires disclosures and controls not just in terms of how data is used but of what data is collected in the first place.

2. TikTok is one of those commercial actors; it has overwhelming incentives to maximize collection of data about users and overwhelming power to do so. Case-in-point is TikTok's collection of data about website users' activity on non-TikTok websites by way of tools like the TikTok Pixel and the TikTok Events API (an abbreviation for Application Programming Interface). TikTok has constructed an essentially inescapable infrastructure for gathering a vast scope of information about the activity of both TikTok users and non-TikTok users on non-TikTok websites.

3. I understand that, almost without exception, TikTok fails to adequately disclose, provide notice of, or obtain consent to its data collection practices to users of websites that incorporate the TikTok Pixel or TikTok Events API.

4. As set forth in this report, an expectation of privacy is prevalent in American society. It exists not only in the real world, but online as well. It extends to consumer's own personal online data, including seven categories of default baseline data taken by TikTok that are identifying and/or sensitive, and demonstrated by Dr. Zubair Shafiq. When TikTok takes this data from non-TikTok users (persons who have, either intentionally or otherwise, not consented to be a member of TikTok), this data gathering violates that expectation of privacy.

II. Case Background

5. Counsel for the Plaintiffs in this action ("Counsel") retained me to develop and provide opinions concerning issues of privacy and the alleged conduct of Defendants, as detailed in this report. My analysis included issues relating to TikTok's disclosures and practices, the TikTok Pixel and Events API at issue, and issues relating to the value of privacy and user data.

6. As I understand it, the case involves the following issues, among others:

- Defendants collect and store personal online data of US individuals that are not registered for the TikTok application ("non-TikTok users").
- TikTok intercepts and collects data while individuals browse non-TikTok websites, such as Etsy, Hulu, Upwork, Sweetwater, Rite-Aid, and others, regardless of whether or not an individual is a TikTok user.
- Defendants collect this data through the TikTok Pixel (installed on websites with no affiliation with TikTok) and through the TikTok Events API (a server-to-server data tracking mechanism similar to the Pixel). The Pixel and/or Events API collect data from approximately 10% to 12% of websites across the Internet. Given this, it is almost impossible for anyone, including non-TikTok users, to avoid TikTok's Pixel or Events

API. Defendants collect this data from websites lacking any disclosed relation or affiliation with Defendants; and, almost without exception, the websites do not disclose that data on their website visitors was collected and sent to TikTok.

7. I understand that the company TikTok, Inc. is closely connected with its Chinese-based parent company ByteDance. Given this relationship, my references to TikTok, will, when appropriate, incorporate ByteDance as well.

8. I understand that the relevant time period for this case is from March 2022 to the present day.

III. Assignment and Methodology

9. I understand that this case involves TikTok's collection, storage, and use of information of non-Tik-Tok users from non-TikTok websites. These are people who have not installed the TikTok app and have not signed up for a TikTok account. Thus, they have not agreed to any terms and conditions set forth by TikTok.

10. I also understand that, for some of the legal claims that Plaintiffs are bringing, Plaintiffs seek to establish that they have a reasonable expectation of privacy regarding their use of websites and that TikTok's collection and use of personal online data from individuals who have never installed the TikTok app, or never signed up for a TikTok account, is highly offensive to a reasonable user.

11. I was asked to opine on the privacy implications of TikTok's data collection.

12. As a first matter, I consider myself to be a neutral party who frequently works with both plaintiffs and defendants in litigation in state and federal courts as well as arbitrations and other litigation-like processes. I employ a consistent set of methodologies regardless of which side has retained me.

13. In preparing my report I have considered the documents identified herein. My opinions are informed in part by publicly available information—that is, news reports, technical bulletins, scientific studies, policy briefs, government documents, and TikTok's public-facing statements. I have had access to filings in this case, including sealed filings. I have had access to documents produced by the parties, transcripts of depositions, and expert declarations and reports created thus far.

14. In my work as an expert, I am often asked to define and explain the terminology used in computer technology. Based on my experience performing this role, I have seen that evidence in litigation often includes technical details that would not make sense to, or would only be partially understood by, the factfinder without explanation by a qualified expert.

15. Based on my expertise, I select appropriate data from reliable sources when tasked with researching technical questions or explaining technical concepts.

16. Finally, I rely upon my educational background and research, as well as my forty years of experience as a cryptography, security, privacy, cybersecurity, and technology engineer, as well

as a writer, teacher, corporate executive, and consultant. I may refer to external works as proper to demonstrate that my opinions are consistent with widely accepted principles and the opinions of other experts.

17. My work is billed at the rate of $1,075 per hour for this case. My compensation does not depend upon my opinions in this matter or the outcome of this litigation.

18. I reserve the right to update my opinions based on any new discovery in this case, which is ongoing and not yet complete. I understand that in August and September 2024, Defendants performed a "document dump", providing over 2.3 million pages of discovery, comprising 86.14% of the total documents produced by document count and 91.30% by page volume. As a result, as of the date of this report, I have not yet had the opportunity to review all the relevant documents that may have produced given such voluminous new available information, especially given the limitations on discovery provided prior to that point.

IV. Expertise

19. My name is Bruce Schneier. I hold an MS Degree in Computer Science, which I obtained from American University in 1986, and a BS Degree in Physics, which I obtained from the University of Rochester in 1984.

20. I work internationally as a technologist. I presently hold the title of Chief of Security Architecture at Inrupt, Inc. From 2016 to 2019, I held the titles of Chief Technology Officer of Resilient Systems, Inc. and then Special Advisor to IBM Security. Prior to that, from 1999 to 2016, I was Chief Technology Officer of Counterpane Internet Security, Inc. and Chief Security Technology Officer of BT. I am also the President of Counterpane Systems LLC, and have been since 1991.

21. I am an Adjunct Lecturer and fellow at the Harvard Kennedy School, where I teach cybersecurity policy. Every spring, I teach a survey course titled "Cybersecurity: Tech, Policy, and Law." Every fall, I teach a seminar module titled "Special Topics in Cybersecurity Policy." Past topics have included AI security, blockchain, election security, and misinformation.

22. I am associated with the Belfer Center for Science and International Affairs and the Ash Center for Democracy and Technology(where I have an office), both at the Harvard Kennedy School. I am also a faculty associate at the Berkman Klein Center for Internet and Society at Harvard University.

23. I serve as board member of the nonprofits Electronic Frontier Foundation and Access Now. I have formerly been a board member of the Electronic Privacy Information Center and the Tor Project. I serve as an advisory board member for the Electronic Privacy Information Center, Verified Voting, and Sightline Security.

24. I am the author of over twelve books on the topics of cryptography, computer security, general security technology, trust, surveillance, and privacy, including *Applied Cryptography* (1994 and 1996), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (2003), *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World* (2015), and *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (2018).

My newest book, *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back*, was published by W.W. Norton in February 2023. I am currently writing a book on AI and democracy, tentatively titled *AI and the New Future of Democracy,* to be published in fall 2025.

25. My work entails the technical aspects of cryptography, computer security, data privacy, Internet security, security technology, surveillance, and AI security. I also research, write and speak about the economic, psychological and sociological aspects of security and privacy. As such, I study user behavior and human factors related to many different aspects of security and privacy. My 2015 book, *Data and Goliath*, discusses people's relationships with privacy, and their behaviors regarding privacy, in detail.

26. I have also authored or coauthored over 100 academic publications on security technology subjects, such as cryptographic design and analysis, security protocol design and analysis, software security, information security, Internet security, security technologies, data privacy, data anonymity, AI security, security policy, privacy policy, cyberespionage, and cyberwarfare.

27. I have published numerous articles on the subject of security technology and its effects at personal, corporate and national levels, for publications such as the *New York Times*, the *Washington Post*, the *Wall Street Journal*, the *Guardian*, the *Atlantic*, *Foreign Policy*, *Forbes*, *Wired*, *Nature*, the *Sydney Morning Herald*, the *Boston Globe*, and the *San Francisco Chronicle.*

28. I have repeatedly testified before Congress on topics of cybersecurity and data privacy.

29. I regularly speak at conferences around the world, both as a paid speaker and pro-bono, often keynoting events.

30. I co-founded the Workshop on Economics and Information Security (now in its twenty-third year) and the International Workshop on Security and Human Behavior (now in its seventeenth year).

31. I am the recipient of many awards, including: (1) Electronic Privacy Information Center Lifetime Achievement Award, 2015; (2) named one of the IFSEC 40: The Most Influential People in Security & Privacy, January 2013; (3) Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011; (4) *CSO* Compass Award, May 2010; (5) Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award, January 2008; (6) Electronic Frontier Foundation Pioneer Award, March 2007; (7) *Dr. Dobb's Journal* Excellence in Programming Award, April 2006; (8) *InfoWorld* CTO 25 Award, April 2005; and (9) Productivity Award for *Secrets and Lies* in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.

32. I am the author of a monthly email newsletter about security, "Crypto-Gram," and the blog "Schneier on Security," which have a combined readership of over 250,000 people.

33. I am a named co-inventor on eighty-two issued US Patents relating to cryptography, computer security, security technology, and electronic commerce.

34. I have spent my entire career focused on issues relating to digital privacy. Before Counsel contacted me about being retained as an expert in this litigation, I was familiar with Internet

surveillance in general, but was unaware of the details of the conduct at issue in this litigation; that is, TikTok's collection and storage of detailed information about non-TikTok subscribers who use non-TikTok websites. It was only through research, including access to Confidential discovery in this litigation, that I understood the extent of these TikTok practices.

35. My detailed CV is included as Appendix 2 to this report. It lists declarations and depositions I have given as an expert witness in recent court cases.

V. Summary of Opinions

36. **One:** An expectation of privacy is prevalent in American society. It is generally recognized that privacy is (1) a basic human need, and (2) crucial for political liberty and justice. This expectation of privacy is elucidated and partly grounded in various literature, including but not limited to legal analysis, statutes, and regulations.

37. **Two:** This expectation of privacy exists not only in the physical world, but online as well. In the years since use of the Internet has become commonplace, norms and regulations have come to recognize this principle.

38. **Three:** This expectation of privacy extends to collection of personal online data, including the seven default categories of sensitive and/or identifying online data taken by TikTok, which is valuable for corporations who collect it. Accordingly, the expectation of privacy (as well as various statutes and regulations) is violated by taking this personal online data from someone without their consent. This is the case for non-TikTok users who have no reason to know that TikTok is taking and using their data.

39. **Four:** Violation of the expectation of privacy becomes particularly offensive when the personal online data taken is sensitive and/or identifying. As demonstrated by Dr. Zubair Shafiq, the data TikTok collects from non-TikTok users is not only valuable to TikTok, but it is also sensitive and/or identifying, in that TikTok collects seven categories of baseline data, from which it can piece together a single user's browsing data from various websites. This data is collected even if a consumer has cookie-blocking enabled. The data collected isn't made materially less sensitive by the fact much of it might be in hashed form. Accordingly, TikTok's methods of data collection, by themselves, raise privacy concerns.

40. **Five:** Violation of the expectation of privacy also becomes particularly offensive when a large amount of personal online data is taken. The data collected by TikTok is of a very high volume, and as the Pixel or Events API are on approximately 10% to 12% of websites, most Americans on the Internet are exposed to the TikTok Pixel and Events API.

41. **Six:** Violation of the expectation of privacy also becomes particularly offensive when an entity collecting the personal online data has a history of privacy violations and/or ties to adversarial governments. Here, TikTok has (1) an affiliation with the Chinese Government, and (2) a history of US-based privacy violations.

VI. Individuals Have a Reasonable Expectation of Privacy on the Internet

1. Privacy

1.1. "Private" and "Privacy" Have Specific Meanings and Implications

42. In today's Internet age, it is important for people to have the option to avoid online surveillance, including by measures as simple as refraining from installing apps known for their surveillance potential.

43. According to the Oxford English Dictionary, the word "privacy" dates back to the 1500s, and refers to "The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion." Privacy consists of freedom from attention by those one can see, and by those one cannot see. With respect to communication, the OED defines "private" as "intended only for or confined to the person or persons directly concerned; confidential."[1]

44. Privacy is linked to the concept of control. In its various official publications, the National Institute of Standards and Technology defines "privacy" as "assurance that the confidentiality of, and access to, certain information about an entity is protected,"2 "the right of a party to maintain control over and confidentiality of information about itself,"3 and "freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual."4 That third definition is also used by the International Organization for Standardization (ISO).5

45. The International Association of Privacy Professionals (IAPP), defines privacy this way: "Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used."[6]

---

[1] *Oxford English Dictionary Online*, "Private" (retrieved September 6, 2024).

[2] Elaine Barker et al., "A framework for designing cryptographic key management systems," NIST Special Publication 800-130, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf (August 2013).

[3] Arthur E. Oldehoeft, "Foundations of a security policy for use of the national research and educational network," NIST IR 4734, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf (February 1992).

[4] Simson L. Garfinkel, "De-identification of personal information," NIST IR 8053, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (October 2015).

[5] International Organization for Standardization, "Information technology: Vocabulary," ISO/IEC 2382:2015, https://www.iso.org/obp/ui/en/#!iso:std:63598:en (May 2015).

[6] International Association of Privacy Professionals, "What is privacy?" https://iapp.org/about/what-is-privacy (2024).

1.2. Privacy Is a Basic Human Need

46. Privacy is central to our ability to control how we relate to the world. Being stripped of privacy is fundamentally dehumanizing, whether it is conducted by an undercover police officer following us around or by computer algorithms and systems tracking our online activities.

47. There is a strong physiological basis for a need for privacy. Biologist Peter Watts makes the point that a desire for privacy is innate: mammals in particular don't respond well to surveillance. Humans consider surveillance a physical threat, as do animals in the natural world who are stalked by predators. Surveillance—defined by the US military as "systematic observation"[7]—makes people feel like prey, just as it makes the surveillors behave like predators.[8]

48. Based on my experience as a technologist with a special interest not only in the technical aspects of privacy but its social and historical context, and not as a lawyer, I understand that the vision of privacy as a fundamental human right is enshrined in both US and international law. It is my understanding as a security and privacy professional that the right to privacy is implied in the Fourth, Fifth, and Ninth Amendments of the US Constitution,[9] and that it is enumerated in the Universal Declaration of Human Rights (1948),[10] the European Convention on Human Rights (1970),[11] and the 2000 Charter of Fundamental Rights of the European Union.[12] I understand that privacy is also a right enshrined in California's Constitution.[13]

49. In 2013, the UN General Assembly approved a resolution titled "The right to privacy in the digital age," affirming that a fundamental right to privacy applies online as well as offline,

---

[7] U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (November 2021).

[8] Peter Watts, "The scorched earth society," Symposium of the International Association of Privacy Professionals, Toronto, Ontario, https://rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf (May 9, 2014).

[9] FindLaw, "Is there a 'right to privacy' amendment?" https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html (last reviewed August 20, 2023).

[10] United Nations, "Universal Declaration of Human Rights," https://www.un.org/en/about-us/universal-declaration-of-human-rights (December 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence").

[11] Council of Europe, "European Convention on Human Rights," https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953) ("Everyone has the right to respect for his private and family life, his home and his correspondence").

[12] European Union, "Charter of Fundamental Rights of The European Union," https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).

[13] Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, and privacy." California Constitution, "Article 1 Declaration of Rights," California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

and that the risk of surveillance undermines this right.[14] The right to privacy recognized by all of these sources informs the normative expectation of ethical software designers that privacy should be protected.

50. One 2013 study found that an increase in users' perceived control over the privacy of their personal information—defined as "40 questions, which varied in intrusiveness about the respondent's life"—is associated with an increased willingness to disclose such information.[15] The study pertained to privacy and data sharing in general, and is relevant when considering TikTok's practice of collecting, saving, and using records of non-TikTok users' activity.

51. Privacy is not a luxury that people value or seek only in times of safety. Instead, privacy is a value to be assiduously preserved at all times. Privacy is essential for liberty, autonomy, and human dignity. Privacy is something to maintain and protect in order for humans to be truly secure. This is something I wrote about extensively in my book *Data and Goliath*.[16]

1.3. Privacy Is Crucial for Political Liberty and Justice

52. It would be incredibly dangerous to live in a world without privacy where, for example, everything a citizen said and did could be stored and brought forward as evidence against them in the future, or made available to companies that wished to construct cradle-to-grave dossiers on individual citizens. The seventeenth-century French statesman Cardinal Richelieu recognized this when he said, "Show me six lines written by the most honest man in the world, and I will find enough therein to hang him." Lavrentiy Beria, head of Joseph Stalin's secret police, declared, "Show me the man, and I'll show you the crime."[17] Both were saying the same thing: if you have gathered enough data about a person, you can find sufficient evidence to make them appear guilty of something, even if they are in fact innocent of wrongdoing.

53. Surveillance leads to self-censorship, which stifles the free exchange of ideas. US Supreme Court Justice Sonia Sotomayor recognized the potential chilling effect of surveillance on society in her concurring opinion in *United States v. Jones*, a 2012 case involving the FBI's installation of a GPS tracker on a defendant's car. Justice Sotomayor wrote: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantity of intimate information about any person whom the

[14] United Nations Office of the High Commissioner for Human Rights, "The right to privacy in the digital age," https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx (2021).

[15] Laura Brandimarte, Alessandro Acquisti and George Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science* 4, no. 3, https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf (May 2013).

[16] Bruce Schneier, *Data and Goliath*, Norton (2015).

[17] Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, https://books.google.com/books/about/Three_Felonies_a_Day.html?id=2xkDvMQlh-YC&source=kp_book_description (2011).

Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[18]

54. Surveillance by commercial entities is no different. When TikTok collects and saves information about individuals—where they have not installed the TikTok app or signed up for a TikTok account—that activity undermines non-TikTok users' privacy and creates risks of surveillance and its ensuing harms.

55. Extensive digital surveillance invites surveillance-based discrimination. A 2014 report by the Obama administration recognized the threat posed by the accumulation and analysis of data on American citizens, noting that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[19]

2. Data Privacy

2.1. People Have Been Denied the Ability to Make Meaningful Internet Privacy Choices

56. Before 1993, the Internet was noncommercial, and "free" was the online norm. When online commercial services first emerged on the Internet, there was a lot of talk about how to charge for them. It quickly became clear that, with some limited exceptions, people at the time were unwilling to pay even a small amount for access. Much like the business model for television, online enterprises turned to advertising as a revenue model, and that revenue model grew phenomenally profitable for those who engaged in surveillance of their users. Advertising platforms can and do charge higher prices for personally targeted advertising than for generally broadcast advertising. Advertising platforms also charge higher prices for advertisements because they can measure the impact of those advertisements on user behavior, a process called conversion tracking. This is how the Internet ended up with a plethora of nominally free websites and mobile apps that collect and sell users' data in exchange for services, then inundate them with advertising.

57. Data privacy is at the heart of public discussions of the rise of "surveillance capitalism." This term was coined by Shoshana Zuboff, professor of psychology at Harvard University, to describe a system that "unilaterally claims human experience as free raw material for translation into behavioral data.... We are the sources of surveillance capitalism's crucial surplus: the objects of a technologically advanced and increasingly inescapable raw-material-extraction operation ... Surveillance capitalist firms...dominate the accumulation and processing of information, especially information about human behavior. They know a great deal about us, but our access to

[18] U.S. Supreme Court, "Decision," *United States v. Jones*, Case No. 10-1259, http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1 (January 23, 2012).

[19] U.S. Executive Office of the President, "Big data: Seizing opportunities, preserving values," https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).

their knowledge is sparse: hidden in the shadow text and read only by the new priests, their bosses, and their machines."[20]

2.2. Privacy Has Become More Important with Widespread Corporate Surveillance

58. US citizens have been harmed by the vulnerability of information collected online and stored by numerous companies. Major data leaks abound. These include:

- Target (2013: 40 million credit and debit records and 70 million customer records stolen in 2013);[21]
- Experian (2015: 15 million T-Mobile account records stolen; 2020: 24 million individual account records and 800,000 business account records stolen; 2021: 220 million account records stolen, representing nearly every citizen of Brazil);[22]
- Yahoo! (2017: 3 billion user account records stolen);[23]
- Marriott Corporation (2018: 383 million booking records, 5.3 million unencrypted passport numbers and tens of millions of encrypted records stolen; 2020: 5.2 million guest records stolen; 2022: 20GB of data stolen, including credit card information and internal company documents);[24]

[20] Shoshana Zuboff, *The Age of Surveillance Capitalism,* Public Affairs, https://openlibrary.org/books/OL26677236M/The_Age_of_Surveillance_Capitalism (2019), pp. 14, 17, 186.

[21] Michael Kassner, "Anatomy of the Target data breach," *ZD Net*, https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned (February 2, 2015).

[22] Jim Finkle, "Massive data breach at Experian exposes personal data for 15 million T-Mobile customers," *Huffington Post*/Reuters, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).

Phil Muncaster, "Experian data breach hits 24 million customers," *InfoSecurity Magazine*, https://infosecurity-magazine.com/news/experian-data-breach-24-million (August 20, 2020).

Brian Krebs, "Experian API exposed credit scores of most Americans," *Krebs on Security*, https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans (April 28, 2021).

Angelica Mari, "Experian challenged over massive data leak in Brazil," *ZD Net*, https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil (February 20, 2021).

[23] Selena Larson, "Every single Yahoo account was hacked—3 billion in all," *CNN Business,* https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (October 4, 2017).

[24] Seena Gressin, "The Marriott data breach," U.S. Federal Trade Commission, https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach (December 4, 2018).

Brandon Vigliarolo, "Marriott Hotels admits to third data breach in 4 years," *The Register*, https://www.theregister.com/2022/07/06/marriott_hotels_suffer_yet_another (July 6, 2022).

- Facebook (2021: 533 million users' phone numbers and other personal data leaked online);[25]
- AT&T (2024: 73 million customer records stolen, including names, phone numbers, addresses, and encrypted passcodes);[26]
- Ticketmaster (2024: 560 million customer records stolen, including credit card numbers and ticket sales information);[27]
- Real Estate Wealth Network (2023: 1.5 billion database records exposed, including information on property owners, sellers and investors; bankruptcies, divorces, tax liens, foreclosures, inheritances, court judgments, etc.);[28] and
- Progress Software (2023: more than 94 million individuals, 2,770 organizations, $15 billion damages from ransomware attacks suffered by users of the MOVEit file transfer application).[29]

59. Smaller but equally notorious incidents such as the 2015 Ashley Madison breach (which exposed 32 million users' personal information) changed the lives of many of its users, and continue to put them at risk.[30]

60. While this particular case doesn't involve a data breach, the data breaches described above demonstrate the legitimacy of concerns that consumers have about having their online data collected by commercial entities. If consumers consent to such data collection, such concerns might be outweighed by the benefits these consumers derive from consenting to data collection. However, no such trade-off exists when, as is the case here, non-TikTok users have not consented to TikTok's data collection, and derive no benefit of any bargain from that data collection.

---

[25] Aaron Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online," *Business Insider*, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (April 3, 2021).

[26] Zack Whittaker, "AT&T won't say how its customers' data spilled online," *TechCrunch*, https://techcrunch.com/2024/03/22/att-customers-data-leak-online (March 22, 2024).

[27] Sopan Deb, "Ticketmaster confirms data breach. Here's what to know," *New York Times*, https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html (May 31, 2024).

[28] Jeremiah Fowler, "1.5 billion records leaked in Real Estate Wealth Network data breach," *Security InfoWatch*, https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach (December 26, 2023).

[29] Zach Simas, "Unpacking the MOVEit Breach: Statistics and Analysis," EmsiSoft, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis (July 18, 2023; updated June 28, 2024).

[30] Zak Doffman, "Ashley Madison hack returns to 'haunt' its victims: 32 million users now watch and wait," *Forbes*, https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait (February 1, 2020).

61. Given the frequency with which these huge troves of data have been compromised, it is not surprising that approximately 80% of respondents to a 2021 Ipsos survey expressed great concern about data privacy and security.[31] Now more than ever, people rightfully seek to use the Internet without being tracked. Some people use privacy-preserving browsers like DuckDuckGo and ad blockers like Privacy Badger and AdBlock Plus, and send their messages using the encrypted Signal app. Some also take simpler measures, such as refraining from installing apps like TikTok that require that users consent to sharing both personal identifying information and information about their online activities.

62. Public concern about privacy has also escalated during the rise of online tracking for purposes of advertising and "website analytics" and "app analytics"—that is, the systematic collection, reporting, and analysis of website and app data for the purpose of understanding site and app usage and maximizing their effectiveness and monetization. This capability has been strengthened with the introduction of SDKs that developers use to build websites and apps, including the TikTok API for Business SDK.

2.3. The EU, As Well as Several US States, Has Passed Comprehensive Data Privacy Laws

63. The implementation of the European Union's General Data Protection Regulation (GDPR)[32] in 2016 precipitated a conspicuous change in the manner in which websites and mobile apps collect data on their users, or allow third parties to collect data on their users. Whereas pre-GDPR, websites usually placed cookies on visitors' browsers without notifying them, and apps gathered various types of data without notifying their users, the new regulation required affirmative notice to and consent by the visitors before their data could be gathered. Although GDPR is in force in the E.U., many US websites and app developers—especially those with many European visitors and customers—have sought to comply with the regulation.

64. The 2018 California Consumer Privacy Act (CCPA)[33] requires both websites and apps to inform users of the sort of information they collect and how it is used, and whether the information is shared and with whom. Users must also be given the opportunity to prohibit the collection of data that could be linked to them or their family.[34] (Note, again, that I am not an attorney nor am I offering a legal opinion, but am commenting regarding the impact of the GDPR and CCPA on privacy and entities' responses to this legislation.)

---

[31] Chris Jackson and Catherine Morris, "Americans report high levels of concern about data privacy and security," *Ipsos,* https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security (March 16, 2021).

[32] European Union, "General data protection regulation (GDPR)," https://gdpr-info.eu (April 27, 2016).

[33] California Consumer Privacy Act, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (effective January 1, 2020).

[34] Joseph J. Lazzarotti and Mary T. Costigan, "CCPA FAQs on cookies," *National Law Review* 13, no. 52, https://www.natlawreview.com/article/ccpa-faqs-cookies (August 29, 2019).

David Zetoony, Christian Auty and Karin Ross, "Answers to the most frequently asked questions concerning cookies and adtech," Bryan Cave Leighton Paisner, https://www.bclplaw.com/print/v2/content/1023613/ccpa-2020-answers-to-the-most-frequently-asked-questions-concerning-cookies-and-adtech.pdf (February 2020).

65. Since then, eighteen other US states have passed comprehensive privacy laws:[35]

- Colorado: Colorado Privacy Act (effective July 1, 2023)[36]
- Connecticut: Connecticut Personal Data Privacy and Online Monitoring Act (effective July 1, 2023)[37]
- Delaware: Delaware Personal Data Privacy Act (effective January 1, 2025)[38]
- Indiana: Indiana Consumer Data Protection Act (effective January 1, 2026) [39]
- Iowa: Iowa Consumer Data Protection Act (effective January 1, 2025) [40]
- Kentucky: Kentucky Consumer Data Protection Act (effective January 1, 2026) [41]
- Maryland: Maryland Online Data Privacy Act (effective October 1, 2025) [42]
- Minnesota: Minnesota Consumer Data Privacy Act (effective July 31, 2025) [43]
- Montana: Montana Consumer Data Privacy Act (effective October 1, 2024) [44]
- Nebraska: Nebraska Data Privacy Act (effective January 1, 2025) [45]
- New Hampshire: SB 255 (effective January 1, 2025) [46]
- New Jersey: SB 332 (effective January 1, 2025) [47]
- Oregon: Oregon Consumer Privacy Act (effective July 1, 2024) [48]

---

[35] Andrew Folks, "US State privacy legislation tracker," International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker (last updated July 22, 2024).

[36] Colorado Privacy Act, https://leg.colorado.gov/bills/sb21-190 (effective July 1, 2023).

[37] Connecticut Personal Data Privacy and Online Monitoring Act, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022 (effective July 1, 2023).

[38] Delaware Personal Data Privacy Act, https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=140388&legislationTypeId=1&docTypeId=2&legislationName=HB154 (effective January 1, 2025).

[39] Indiana Consumer Data Protection Act, https://iga.in.gov/pdf-documents/123/2023/senate/bills/SB0005/SB0005.05.ENRH.pdf (effective January 1, 2026).

[40] Iowa Consumer Data Protection Act, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262 (effective January 1, 2025).

[41] Kentucky Consumer Data Protection Act, https://apps.legislature.ky.gov/law/acts/24RS/documents/0072.pdf (effective January 1, 2026).

[42] Maryland Online Data Privacy Act, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0541 (effective October 1, 2025).

[43] Minnesota Consumer Data Privacy Act, https://www.revisor.mn.gov/bills/text.php?number=HF4757&type=bill&version=4&session=ls93&session_year=2024&session_number=0&format=pdf (effective July 31, 2025).

[44] Montana Consumer Data Privacy Act, https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf (effective October 1, 2024).

[45] Nebraska Data Privacy Act, https://nebraskalegislature.gov/bills/view_bill.php?DocumentID=54904 (effective January 1, 2025).

[46] New Hampshire SB 255, https://gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1 (effective January 1, 2025).

[47] New Jersey SB 332, https://www.njleg.state.nj.us/bill-search/2022/S332 (effective January 15, 2025).

- Rhode Island: Rhode Island Data Transparency and Privacy Protection Act (effective January 1, 2026) [49]
- Tennessee: Tennessee Information Protection Act (effective July 1, 2025) [50]
- Texas: Texas Data Privacy and Security Act (effective July 1, 2024) [51]
- Utah: Utah Consumer Privacy Act (effective December 31, 2023) [52]
- Virginia: Virginia Consumer Data Protection Act (effective January 1, 2023)[53]

66. Michigan,[54] Ohio[55] and Massachusetts[56] have privacy bills being debated in committee.

67. Thirty-nine privacy-related pieces of federal legislation have been introduced in the 118th Congress (2023–2024). These bills pertain to consumer privacy, workplace privacy, financial privacy, health privacy, children's and educational privacy, and governmental privacy obligations.[57]

68. These myriad pieces of legislation demonstrate that legislators recognize the expectation of privacy applies to Internet usage.

3. Personal Online Data

3.1. Browsing Information Can Be Highly Revealing

69. Non-TikTok users who have chosen not to install the TikTok app have not consented to TikTok's collection of any of their online activity and associated content, whether others might regard that activity as sensitive or not.

---

[48] Oregon Consumer Privacy Act, https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled (effective July 1, 2024).

[49] Rhode Island Data Transparency and Privacy Protection Act, https://fpf.informz.net/z/cjUucD9taT00MjA3NjkzJnA9MSZ1PTQzNzQ3OTU0MCZsaT00Njk5MDQ2Mw/index.html (effective January 1, 2026).

[50] Tennessee Information Protection Act, https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073 (effective July 1, 2025).

[51] Texas Data Privacy and Security Act, https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB4 (effective July 1, 2024).

[52] Utah Consumer Privacy Act, https://le.utah.gov/~2022/bills/static/SB0227.html (effective December 31, 2023).

[53] Virginia Consumer Data Protection Act, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (effective January 1, 2023).

[54] Michigan Personal Data Privacy Act (SB 1182), https://legislature.mi.gov/Bills/Bill?ObjectName=2022-SB-1182 (introduced September 27, 2022).

[55] Ohio Personal Privacy Act (HB 376), https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA134-HB-376 (introduced July 12, 2021).

[56] Massachusetts Data Privacy Protection Act (Bill S.2770) in, https://malegislature.gov/Bills/193/S2770.pdf (introduced February 16, 2023; revised bill submitted May 9, 2024).

[57] Müge Fazlioglu, "U.S. federal privacy legislation tracker," International Association of Privacy Professionals, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker (last updated August 2024).

70. Among the first services that Internet users are likely to encounter are web browsers. A user's search history can go back many years; in the case of users under 30, it may encompass most of their lifespan. In addition, websites often place cookies on users' systems to help track their search history. As demonstrated below, this collection of such information is vast and can track information deemed sensitive by those users.

71. A 2013 study of 368,284 users of both desktop and mobile devices detected a unique browsing history for 69% of participants, and found that out of users for whom at least four visited websites were detected, 97% could be uniquely identified by their browsing history.[58]

72. A 2015 research paper illustrated how third-party cookies can be used by eavesdroppers—these are people who are not the owners of the websites visited, apps used or cookies—to track people on the Internet. Simulating users browsing the web, the authors found that "the adversary can reconstruct 62–73% of a typical user's browsing history."[59] Advertising identifiers, like cookies, identify a device, and can therefore be used for similar purposes.

73. Data collected from users' online activity (and then saved by either developers or third parties) can have real-world consequences, given changing federal and state laws. For example, the US Supreme Court's 2022 decision to overturn *Roe v. Wade* and concurrent efforts in numerous states to criminalize abortion have precipitated concern about the extent to which online data could be used as evidence against women who obtain abortions. Given that browser history has been used as evidence in prosecutions of women who have sought to terminate a pregnancy,[60] concern about the inappropriate use of data pertaining to one's reproductive function is reasonable.

74. Dr. Shafiq has determined that TikTok collects information from non-TikTok users that can be used to infer sensitive information such a home/work address, gender, age, marital status, educational background, occupation, religious, political, and sexual associations. Dr. Shafiq also notes that browsing history is highly identifying .[61] (I understand that Dr. Shafiq will submit a further expert report on the same date as my expert report. I reserve the right to review and rely upon Dr. Shafiq's expert report in addition to his previous declarations.)

---

[58] Lukasz Olejnik, Claude Castelluccia and Artur Janc, "Why Johnny can't browse in peace: On the uniqueness of web browsing history patterns," *Annals of Telecommunications* 1-2, https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf (June 2013).

[59] Steven Englehardt, et al., "Cookies that give you away: The surveillance implications of web tracking," *WWW '15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).

[60] Cat Zakrzewski, Pranshu Verma and Claire Parker, "Texts, web searches about abortion have been used to prosecute women," *Washington Post*, https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution (July 3, 2022).

[61] Expert Reply Declaration of Zubair Shafiq Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated July 26, 2024 ("Shafiq Reply Decl.") at ¶¶ 85-94. I understand that Dr. Shafiq will submit a further expert report on the same date as my expert report. I reserve the right to review and rely upon Dr. Shafiq's expert report in addition to his previous declarations.

3.2. Personal Data Generates Billions in Corporate Revenue

75. The largest online companies have powerful incentives to capitalize on consumers' data to generate billions in revenue. Together, Google and Facebook dominate this field: in 2022, Google took in $224.473 billion in digital advertising revenue,[62] and Facebook $113.642 billion.[63] The much smaller but much more rapidly growing TikTok took in $13.2 billion in US ad revenue in 2023, representing 3.4% of US digital ad expenditures.[64] These revenues are tied to data-driven advertising.

76. Other problems arise when commercial entities treat their underlying algorithms as trade secrets: TikTok's recommendation algorithms and credit-scoring systems are two examples. Companies that use proprietary algorithms have legitimate concerns about trade secrecy. They're worried that competitors will copy them and that people will figure out how to game them. But this secrecy prevents transparency, which is critical when the algorithms in question have a direct impact on the public.[65] As discussed in detail below, TikTok collects data from both TikTok members and non-TikTok users for its own financial benefit, including to refine its recommendation and ad bidding algorithms, but there is limited information available in terms of what that means for internet users' privacy.

77. Consumer surveillance is much older than the Internet. Before the Internet, there were four basic surveillance streams. The first flowed from companies keeping records on their own customers. The second stream flowed from direct mail marketing, which involved the creation of lists of prospects who might welcome a vendor's promotional or fundraising mail so that time, money, materials, and effort would not be spent to solicit those who would be unreceptive. Direct mail lists were sorted according to demographic characteristics; many had their beginnings as aggregated magazine subscription lists, or customer lists from related enterprises.

78. The third surveillance stream came from credit bureaus, which collected detailed information about individuals' financial transactions, and sold that information to banks needing to determine the creditworthiness of potential customers. This detailed, expensive form of data collection was only cost-effective for high-risk matters such as credit card approvals, apartment leases, mortgages, and the like.

79. The fourth surveillance stream flowed from the government. This stream consisted of public records: birth and death certificates, driver's license records, voter registration records, various permits and licenses, court documents, and so on. Private enterprises have increasingly

---

[62] Alphabet, Inc., "Form 10-K," United States Securities and Exchange Commission, https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf?cache=5ae4398 (February 3, 2023).

[63] Meta Platforms, Inc., "Form 10-K," United States Securities and Exchange Commission, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf (February 3, 2023).

[64] Sara Lebow, "Guide: TikTok," Emarketer. https://www.emarketer.com/insights/guide-tiktok (July 18, 2024).

[65] Frank Pasquale, "The troubling trend toward trade secret-protected ranking systems," Chicago Intellectual Property Colloquium, Chicago, Illinois, https://blogs.kentlaw.iit.edu/wp-content/uploads/sites/36/files/2016/12/pasquale.pdf (April 21, 2009).

been able to acquire or purchase this public data for their own use; use cases include people-search websites, websites featuring arrest records, and real estate websites.[66]

80. Credit bureaus and direct marketing companies eventually combined these four streams, evolving into modern-day data brokers like Acxiom.[67] Data brokers buy citizens' personal data from private businesses, combine it with publicly available information about them, and sell the results to entities willing to pay the price. And they've ridden the tides of computerization. The more data an individual produces, the more information about them can be collected and the more accurately they can be profiled, leading to still greater revenues for companies that aggregate and market citizens' personal information.[68]

81. While some businesses seek data about other businesses' customers, the context is very different when a third party is collecting data flows from individual computers, phones, or tablets of the first party's customers.

82. A 2016 analysis of the history of Internet tracking between 1996 and 2016 found that it has become more prevalent, more complex, and more difficult to avoid, and that trackers capture an increasing range of users' online behaviors while using browsers and other mobile apps.[69]

83. The 2016 implementation of the European Union's General Data Protection Regulation precipitated a conspicuous change in the manner in which websites and mobile apps collected data on their users, or allowed third parties to collect data on their users. Whereas pre-GDPR, websites usually placed cookies on visitors' browsers without notifying them, and apps gathered various types of data without notifying their users, the new regulation required affirmative notice to and consent by the user before their data can be gathered. Although GDPR is in force in the E.U., many US websites and app developers—especially those with many European visitors and customers—have sought to comply with the regulation.

84. The 2018 California Consumer Privacy Act requires both websites and apps to inform users of the sort of information they collect and how it is used, and whether the information is shared and with whom. Users must also be given the right to opt out the collection of data that

---

[66] Amy Harmon, "As public records go online, some say they're too public," *New York Times*, https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html (August 24, 2001).

Mark Ackerman, "Sales of public data to marketers can mean big $$ for governments," CBS Denver, https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments (August 26, 2013).

[67] Natasha Singer, "Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome," *New York Times*, https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html (June 16, 2012).

[68] Craig Timberg, "Brokers use 'billions' of data points to profile Americans," *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

[69] Adam Lerner, et al., "Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016," 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner (2016).

could be linked to them or their family.[70] (Note, again, that I am not an attorney nor am I offering a legal opinion, but am commenting regarding the impact of the GDPR and CCPA on privacy and entities' responses to this legislation.)

85. Commercial entities that collect user data must focus not only on collection (subject to restrictions on the timing of collection) but also on the appropriate use of data, and its retention and deletion. When storage was expensive, businesses had an incentive to minimize collection, purge useless data, and enforce time limits for data retention in order to minimize the cost of data storage. However, storage is now cheap, thus increasing the risk that companies will retain data far longer than is needed for the successful conduct of business; and the commodification of data translates into business opportunities for those enterprises willing to part with it.

86. Protecting privacy requires regulation in many places: at collection, during storage, upon use, during disputes. The OECD Privacy Framework, adopted in 1980, delineates a set of basic principles of data privacy protection that illustrate the scope of this need:

> COLLECTION LIMITATION PRINCIPLE: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> DATA QUALITY PRINCIPLE: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> PURPOSE SPECIFICATION PRINCIPLE: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> USE LIMITATION PRINCIPLE: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.
>
> SECURITY SAFEGUARDS PRINCIPLE: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> OPENNESS PRINCIPLE: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

---

[70] Joseph J. Lazzarotti and Mary T. Costigan, "CCPA FAQs on cookies," *National Law Review* 13, no. 52, https://www.natlawreview.com/article/ccpa-faqs-cookies (August 29, 2019).

David Zetoony, Christian Auty and Karin Ross, "Answers to the most frequently asked questions concerning cookies and adtech," Bryan Cave Leighton Paisner, https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf (February 2020).

> INDIVIDUAL PARTICIPATION PRINCIPLE: Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> ACCOUNTABILITY PRINCIPLE: A data controller should be accountable for complying with measures which give effect to the principles stated above.[71]

87. The ACM Code of Ethics and Professional Conduct (which TikTok, as an employer of computer scientists, should be aware of in formulating its course of conduct) speaks to similar effect.

> 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
>
> This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and ***privacy***. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority. [*emphasis added*]
>
> 1.3 Be honest and trustworthy.
>
> Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.
>
> 1.6 Respect privacy.
>
> The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing

[71] Organization for Economic Cooperation and Development, "The OECD privacy framework," http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

> professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.
>
> Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.
>
> Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.[72]

88. In its 2018 "Statement on the Importance of Preserving Personal Privacy," the ACM outlined a series of "Foundational Privacy Principles and Practices," including:

> Ensure that communications with individuals (i.e., data subjects) are comprehensible, readable, and straightforward.
>
> Ensure that individuals are able to prevent personal data obtained for one purpose from being used or made available for other purposes without that person's informed consent.[73]

The GDPR's Principles state that personal data must be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical

[72] Association for Computing Machinery, "ACM code of ethics and professional conduct," https://www.acm.org/code-of-ethics (June 22, 2018).

[73] Association for Computing Machinery, U.S. Public Policy Council, "USACM statement on the importance of preserving personal privacy," https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf (March 1, 2018).

purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[74]

4. Individual Attitudes Towards Privacy

4.1. People's Privacy Intuition Is Suited to Face-To-Face Interactions

89. People reveal data about themselves all the time: to family, friends, acquaintances, lovers, even strangers. They share personal information with doctors, investment counselors, and psychologists. They share a lot of data. But they usually think of that sharing transactionally: "I'm sharing data with you, because I need you to know things/trust you with my secrets/am reciprocating because you've just told me something personal." That sharing usually occurs in the context of face-to-face encounters, in which people are typically in control and aware of what they are sharing, and aware of the identity of the parties they are sharing it with.

90. Humans are social animals, and there are few things more powerful or rewarding to humans than communicating with other people. Digital means have become the easiest and quickest way to communicate; they have functioned as a lifeline for millions of people sequestered in their homes during the pandemic. However, trading privacy for services isn't necessarily a good or fair bargain, at least as these bargains are structured today, absent comprehensive federal legislation comparable to Europe's GDPR. Users may inadvertently accept invidious deals presented in opaque, frequently modified privacy policies, and whose terms they do not fully understand or are never adequately disclosed at all.

91. This lack of transparency makes it hard for people to make complex privacy decisions about the browsers they use, websites they visit, apps they install on their smartphones, and the amount of personal information they disclose via all of these means.

[74] European Commission, "General Data Protection Regulation: Art. 5 GDPR: Principles relating to processing of personal data," https://gdpr-info.eu/art-5-gdpr (enacted April 5, 2016; effective May 25th, 2018).

92. Continual exposure of their data online cannot serve as evidence of their consent to be monitored, especially when they seek to affirmatively protect their privacy by declining to use apps like TikTok or by other means.

VII. Individuals Have a Reason to Avoid Surveillance by TikTok

5. TikTok has a Surveillance-Dependent Business Model

5.1. The TikTok Pixel and Events API Contribute to a Significant Revenue Source for TikTok

93. TikTok currently leads the pack in its ad revenue growth rate. In the second quarter of 2023, ByteDance (the company that owns TikTok) posted $29 billion in worldwide revenues, representing an increase of 40% over the preceding year; $5.8 billion of those second-quarter revenues came from TikTok users outside China. In comparison, during the same period, Meta's revenues rose by 11%.[75]

94. TikTok collects data from activity on non-TikTok websites and apps by way of the TikTok Pixel.

95. TikTok's data collection is enabled in large part to the company's free provision of its app to a user base that now numbers one billion worldwide; its free provision of TikTok Business Accounts, which enable advertisers and developers to freely activate and view TikTok Analytics; its free provision of the TikTok Pixel and/or Events API to developers; and its free provision of an in-app browser, creating a first-party pipeline to web browsing activity.

96. As detailed below, many private organizations and public agencies have begun to question the wisdom of using TikTok products because of the company's retention of individual user data for its advertising enterprise, and the difficulty of obtaining truly informed consent from non-TikTok users who are not fully apprised of the specific data they are being asked to share.[76]

5.2. Non-TikTok Da Coll cte i k ix d ven API

[redacted]

[redacted]

[redacted]

[75] Daniel Konstantinovic, "ByteDance revenues rival Meta as both compete over social commerce," *eMarketer*, https://www.emarketer.com/content/bytedance-revenues-rival-meta-both-compete-over-social-commerce (November 15, 2023).

[76] Ryan Barwick, "Advertisers are asking questions about the data TikTok can collect," *Marketing Brew*, https://www.marketingbrew.com/stories/2022/11/22/advertisers-are-asking-questions-about-the-data-tiktok-can-collect (November 22, 2022).

Sumeyya Ilanbey and David Swan, "Australian companies dump TikTok tracking tool amid privacy concerns," *Sydney Morning Herald*, https://www.smh.com.au/business/companies/australian-companies-dump-tiktok-tracking-tool-amid-privacy-concerns-20240110-p5ewc0.html (January 15, 2024).

b. [redacted]

100. TikTok also offers a free software development kit (TikTok API for Business SDK) to website and app developers that developers can use to build and monetize their apps. TikTok uses these services to surveil every user of a website or app that integrates its Pixel and/or Events API, without making clear to developers that there is no setting that would allow their website's visitors to escape this surveillance, and without directly offering individuals using such sites the opportunity to opt out.

101. [redacted]

[77] Defendants' Amended Responses and Objections to Plaintiffs' Interrogatory No. 8; Dan Kirshgessner Transcript, April 17, 2024, pp. 92–98.

[78] TIKTOK-BG-000002930–940 at 934–935.

[79] *Id.* at 938.

[80] *Id.* at 932.

[81] *Id.*

[82] Lizzie Li Transcript, June 5, 2024, at 215:2-20.

[redacted][83]

6. The Data Collected by the TikTok Pixel and Events API Causes Significant Privacy Risk

6.1. It is Practically Impossible to Avoid the TikTok Pixel or Events API while Using the Internet

102. From its headquarters in California, TikTok has established massive data centers around the world to power its app and data storage operations, and to accumulate and organize the information submitted and generated by both TikTok users and non-TikTok users that powers its advertising operations.

103. TikTok was introduced in the US in 2018, and in 2020, 2021, and 2022 was the most downloaded app in both the US and the world.[84] TikTok is now the world's fourth largest social media platform, with over one billion users per month worldwide. The app has been installed over three billion times since its introduction in 2016, and is available in the vast majority of countries. One-fifth of the world's 4.8 billion Internet users use TikTok. The US currently has the world's largest TikTok audience, with over 150 million installations of the app, and over 102 million users per month engaging with it.[85] Approximately half the USUS population uses TikTok.[86] Currently, 18-24 year olds in the US spend an average of 76 minutes per day on the TikTok platform.[87]

104. The TikTok Pixel and Events API is incorporated into many heavily-used websites. A 2023 study by Canadian cybersecurity firm Feroot Security found TikTok tracking pixels on approximately 10% of the 3,500 sites it visited, including 30 US state government websites in 27 states.[88]

105. A December 2022 study found that many online healthcare apps and websites were leaking medical information they collected to advertising platforms, including information about their customers' prescription purchases and treatment plans. Nearly half of the platforms tested

---

[83] Defendants' Responses and Objections to Plaintiffs' Interrogatory No. 24.

[84] Sapna Maheshwari, "Love, hate or fear it, TikTok has changed America," *New York Times*, https://www.nytimes.com/interactive/2024/04/18/business/media/tiktok-ban-american-culture.html (April 19, 2024).

[85] Matthew Woodward, "TikTok user statistics: Everything you need to know," *Search Logistics*, https://www.searchlogistics.com/learn/statistics/tiktok-user-statistics (May 31, 2024).

[86] Sapna Maheshwari, "Love, hate or fear it, TikTok has changed America," *New York Times*, https://www.nytimes.com/interactive/2024/04/18/business/media/tiktok-ban-american-culture.html (April 19, 2024).

[87] Minda Smiley, "Social time spent by Generation Z," *eMarketer*, https://www.emarketer.com/content/social-time-spent-by-generation-2024 (March 29, 2024).

[88] Byron Tau and Duston Volz, "U.S. state-government websites use TikTok trackers, review finds," *Wall Street Journal*, https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0 (March 21, 2023).

contained the TikTok Pixel.[89] In March 2023, mental health telehealth startup Cerebral admitted that since the company's inception in 2019 it had shared more than 3.1 million users' mental health assessments and other private information with advertisers and tech companies, including TikTok.[90]

106. In early 2024, researchers at Lokker, a data privacy consultancy, analyzed 3,419 US websites in the healthcare, technology, financial services and retail fields, as well as the S&P 500, and found that 12% of websites across all industries, including 9% of S&P 500 companies and 4% of healthcare companies, contained the TikTok Pixel.[91]

107. These third-party platforms transmit to TikTok user data collected for functions such as displaying ads within TikTok, logging in and displaying videos on their own websites and apps. Even more apps and websites embed TikTok tracking pixels that transmit information about users' and non-TikTok users' page visits and activity. Although a TikTok spokesperson insisted that TikTok SDKs are used to "share" rather than "collect" data, and that advertisers, not TikTok, are responsible for specifying the sorts of data sent to them, the distinctions are disingenuous and immaterial. Once data resides on TikTok's servers, it is in the company's possession.[92]

108. In September 2022, a Consumer Reports investigation found that hundreds of organizations—including the United Methodist Church, Weight Watchers, the Arizona Department of Economic Security, Planned Parenthood, Girl Scouts, RiteAid, WebMD, Recovery Centers of America, and the College Board—embedded the TikTok Pixel, which automatically notifies TikTok of their visitors' IP addresses, unique ID number, pages visited, clicks, types, searches and other events. If a child visits the Girl Scouts site, data about the visit is transmitted to TikTok. If a visitor searches for "erectile dysfunction" on WebMD, TikTok is immediately informed about it. If a shopper adds Plan B emergency contraceptives to their RiteAid cart, TikTok sees it. If an alcoholic or drug addict searches for information on Recovery Centers of America facilities or insurance coverage, TikTok gets the data.[93]

109. A September 2024 FTC report on the data practices of social media and online video companies found that "the tech industrys monetization of personal data has created a market for

---

[89] Todd Feathers, Katie Palmer and Simon Fondrie-Teitler, "'Out of control': Dozens of telehealth startups sent sensitive health information to Big Tech companies," *The Markup*, https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (December 13, 2022).

[90] Zack Whittaker, "Telehealth startup Cerebral shared millions of patients' data with advertisers," *TechCrunch*, https://techcrunch.com/2023/03/10/cerebral-shared-millions-patient-data-advertisers (March 10, 2023).

[91] LOKKER, "Website privacy and compliance challenges: Qualifying website privacy risks," https://lokker.com/wp-content/uploads/2024/04/LOKKER_Online-Data-Privacy-Report_032024-2.pdf (March 2024).

[92] Thomas Germain, "We found 28,000 apps sending TikTok data. Banning the app won't help," *Gizmodo*, https://gizmodo.com/tiktok-ban-joe-biden-28000-apps-sdk-data-china-1850174019 (March 2, 2023).

[93] Thomas Germain, "How TikTok tracks you across the web, even if you don't use the app," *Consumer Reports*, https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813 (September 29, 2022).

commercial surveillance [...] with inadequate guardrails to protect consumers," and that "Companies engaged in mass data collection of their users and in some cases non-users." The FTC characterized the use of tracking pixels as "privacy-invasive"; noted that both "user and non-user information was, by default, ingested into and used by Algorithms, Data Analytics, or AI," but that "users and non-users likely did not know, did not understand, and did not control the wide-ranging collection and uses of their data"; and decried the fact that both users and non-users of these platforms "lacked any meaningful control" over how their personal information was used to fuel these systems.[94]

110. As noted by Dr. Shafiq, given the prevalence of TikTok's Pixel, over the course of one year, it is almost certain that a non-TikTok user with average Internet viewing habits would have the Pixel collect [redacted].[95]

111. Given TikTok's ambitious and phenomenal growth, and the extraordinary range of information that the company accumulates about its users and non-TikTok users, TikTok's data collection practices (including its collection of data from persons who have never installed the TikTok app) can be characterized as a form of pervasive monitoring; that is, "widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers.... [Pervasive monitoring] is distinguished by being indiscriminate and very large scale... [Pervasive monitoring] is an attack on the privacy of Internet users and organisations."[96]

6.2. TikTok Collects Sensitive And/Or Identifying Personal Online Data From Non-TikTok Users

112. I understand that, since at least March 2022, TikTok automatically collects the following seven categories of data from non-TikTok users: (1) Timestamp, (2) IP Address, (3) User Agent, (4) Cookies, (5) URL, (6) what Dr. Shafiq describes as Event Information, and (7) what he describes as "Content Information."[97]

113. I understand that Dr. Shafiq's testing has confirmed that the first six of these data categories uniformly collected, and for Content Information, data is collected in 95.8% to 99.8% of instances.[98] I understand that Dr. Shafiq's testing demonstrates that the browser used by non-TikTok users makes no difference in automatically collecting data through the Pixel.[99]

---

[94] U.S. Federal Trade Commission, "A look behind the screens: Examining the data practices of social media and video streaming services," https://www.ftc.gov/reports/look-behind-scenes-examining-data-practices-social-media-video-streaming-services (September 19, 2024).

[95] Shafiq Reply Decl. at ¶¶ 83-84.

[96] Stephen Farrell and Hannes Tschofenig, "Pervasive monitoring is an attack," *Best Current Practice* 188, Internet Engineering Task Force, https://datatracker.ietf.org/doc/html/rfc7258 (May 2014).

[97] Declaration of Zubair Shafiq Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated June 21, 2024 at ¶ 59-65.

[98] *Id.* at ¶ 84.

[99] *Id.*

6.3. "Hashing" of Collected Data Does Very Little to Mitigate the Privacy Risk

114. TikTok's Privacy Policy discloses that its customers share "mobile identifiers for advertising, hashed email addresses and phone numbers, and cookie identifiers," and that TikTok collects "similar information directly from their websites that integrate TikTok Advertiser Tools (such as TikTok Pixel)."[100] Hashing involves the mathematical transformation of a piece of data, such as an email address, phone number or Social Security number, into a number called a "hash." Although the TikTok Privacy Policy implies that hashing somehow preserves user privacy, the FTC warns, "While hashing might obscure how a user identifier appears, it still creates a unique signature that can track a person or device over time."[101]

115. This is consistent with Dr. Shafiq's analysis, which notes that hashed email addresses and phone numbers can be trivially reversed and linked to an individual, for as little as four to eight cents.[102] Dr. Shafiq has advised that "hashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized."[103]

6.4. The Volume of Data Collected by TikTok Is Tremendous

116.

117. The Pixel and Events API are also on an alarming number of websites. As discussed previously, and at greater length by Dr. Russell W. Mangum III, studies performed by software

---

[100] TikTok, "Privacy policy," https://www.tiktok.com/legal/privacy-policy-row (last updated August 19, 2024).

[101] U.S. Federal Trade Commission, "No, hashing still doesn't make your data anonymous," https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous (July 24, 2024).

Ed Felten, "Does hashing make data 'anonymous'?" Federal Trade Commission, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous (April 22, 2012).

[102] Shafiq Reply Decl. at ¶ 79.

[103] *Id.*

[104] TIKTOK-BG-000736841, at 843 (emphasis in original)

[105] See e.g. TIKTOK-BG-000217358, at 360

[106] See e.g. TIKTOK-BG-000746271, at 272 (policy of trying to get both Pixel and Events API, using a "full funnel" approach).

privacy and security firms Feroot and LOKKER have estimated that approximately 10% to 12% of websites use the TikTok Pixel.[107]

6.5. TikTok Fails to Provide Adequate Notice or Obtain Non-TikTok Users' Consent

118. It is undisputed that consumers very rarely read websites privacy policies and terms of use. This is because the opportunity costs of reading each one greatly outweigh the benefits. For example, empirical data shows that it would take seventy-six work days to read the privacy policies the average citizen encounters in a year.[108]

119. In fact, many consumers are confused by the concept of a "privacy policy" The phrase "privacy policy" alone implies a policy that would protect users from such an abusive misuse of their private data.[109]This misuse of private information is also contrary to the assertions in many privacy policies to the effect of "[w]e are committed to protecting and respecting your privacy."

120. Even assuming for the sake of argument that each consumer reads and understands each privacy policy or Terms of Use for each website, I understand that very few, if any, websites specifically disclose that they used TikTok's Pixel or Events API use in these documents.

121. My understanding is that, while TikTok, in its agreement with advertisers, requires them to "provide[] all necessary transparency notices, and have all necessary rights, permissions and lawful bases (including consent, if and where required) required by applicable laws",[110] TikTok fails to enforce this. [redacted]

[107] Declaration of Russell W. Mangum III, Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated June 21, 2024, at ¶¶ 117-19.

Todd Feathers, Katie Palmer and Simon Fondrie-Teitler, "'Out of control': Dozens of telehealth startups sent sensitive health information to Big Tech companies," *The Markup*, https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (December 13, 2022) (discusses analysis by Feroot Security).

LOKKER, "Website privacy and compliance challenges: Qualifying website privacy risks," https://lokker.com/wp-content/uploads/2024/04/LOKKER_Online-Data-Privacy-Report_032024-2.pdf (March 2024).

[108] Helen A.S. Popkin, "Life is too short to read privacy policies - here's statistical proof!" NBC News, https://www.nbcnews.com/tech/tech-news/life-too-short-read-privacy-policies-heres-statistical-proof-flna297399 (March 2, 2012).

[109] E.E. Hutchinson, "Keeping your personal information personal: Trouble for the modern consumer," 43 Hofstra L.Rev. 1151, 1168, https://scholarlycommons.law.hofstra.edu/hlr/vol43/iss4/7 (January 1, 2015). (citing empirical data showing that "seventy-five percent of (Internet) users believed that '[w]hen a website has a privacy policy, it means the site will not share [their] information with other websites and companies").

[110] TikTok, "TikTok Business Products (Data) Terms," https://ads.tiktok.com/i18n/official/policy/business-products-terms (effective July 29, 2024).

[111] TIKTOK-BG-000009045, at 52.

7. TikTok's Affiliation with the Chinese Government and History of US-Based Privacy Violations Heightens the Risk

7.1. TikTok Has a History of Privacy Violations

122. TikTok's history of privacy concerns in other areas demonstrates TikTok's cavalier attitude towards privacy, and thus raises privacy concerns for non-TikTok users here.

123. In February 2019, the FTC fined TikTok $5.7 million—then the largest civil penalty for violations of the Children's Online Privacy Protection Act (COPPA) for Musical.ly's collection and display of personal information of preteen children, including full names, profile pictures, and biographical information. Further, profiles were public by default; profiles set to private still displayed photos and biographies, and could receive direct messages from unknown parties. Although the violations occurred before TikTok's 2018 acquisition of Musical.ly, TikTok was held legally responsible.[112]

124. In 2019, security researchers discovered that the TikTok app bypassed safeguards built into the Android operating system in order to collect users' unique mobile device identifiers (the MAC address) so that it could surreptitiously track them online, regardless of their privacy choices. Google banned the practice after discovering it. Evidence was later found that TikTok was "able to avoid code audits on the Apple and Google app stores. [TikTok] is capable of changing the app's behavior as it pleases without users' knowledge and utilizes device tracking that essentially gives the company and third parties an all-access pass to user data."[113]

125. In August 2020, security researchers located an unsecured database containing profile data from 42 million TikTok accounts, as well as over 191 million Instagram users and nearly 4 million YouTube users. The researchers determined that the trove was the creation of Deep Social, a company banned by Facebook and Instagram in 2018 for scraping user profile data.[114]

126. In August 2020, twenty lawsuits filed against TikTok in the preceding year were consolidated into a class action, alleging that the app collected minor users' biometric, location and contact information, impermissibly sold the data to advertisers, and sent it to data servers in China.[115] Plaintiffs included residents of California, where TikTok is based, and Illinois, whose

---

[112] U.S. Federal Trade Commission, "Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law," https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy (February 27, 2019).

[113] Antoinette Siu, "TikTok can circumvent Apple and Google privacy protections and access full user data, 2 studies say (Exclusive)," *Yahoo! News*, https://www.yahoo.com/entertainment/tiktok-circumvent-apple-google-privacy-140000271.html (February 14, 2022).

[114] Paul Bischoff, "Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and Youtube," *Comparitech*, https://www.comparitech.com/blog/information-security/social-data-leak (May 30, 2021).

Davey Winder, "235 million Instagram, TikTok and YouTube user profiles exposed in massive data leak," *Forbes*, https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=3a1f04331111 (August 19, 2020).

[115] Bobby Allyn, "Class-action lawsuit claims TikTok steals kids' data and sends it to China," National Public Radio, https://www.npr.org/2020/08/04/898836158/class-action-lawsuit-claims-tiktok-steals-kids-data-and-sends-it-to-china (August 4, 2020).

Biometric Information Privacy Act requires written consent for the collection of biometric information. TikTok denied any wrongdoing, but agreed to settle the suit six months later for $92 million, payable to 89 million TikTok users in the US[116] After this suit was filed, TikTok changed the terms of its privacy policy to require users to consent to the collection of their "biometric identifiers and biometric information...such as faceprints and voiceprints."[117]

127. In March 2022, California's Attorney General announced a nationwide investigation into TikTok in order to determine whether "techniques utilized by TikTok to boost young user engagement, including strategies or efforts to increase the duration of time spent on the platform and frequency of engagement with the platform," are associated with physical and mental health harms to young users.[118]

128. In 2022, researchers at Radboud University discovered that although TikTok stated that its "automatic advanced matching" function would trigger data collection upon submission of a form, TikTok Pixels on 154 US sites and 147 sites in the EU were grabbing hashed email addresses from forms in response to clicks on any links or buttons on the page other than the submit button; that is, the TikTok Pixel collects hashed personal information even when a user abandons a form and navigates away from a page. This behavior is not inadvertent; TikTok's JavaScript code doesn't attempt to recognize "submit" buttons or "submit" events.[119]

U.S. District Court for the Northern District of California, First amended complaint, *Misty Hong, et al., v. Bytedance, Inc., TikTok, Inc., et al*, Case 5:19-cv-07792-LHK, https://s3.documentcloud.org/documents/7012757/TikTok-MDL.pdf (May 11, 2020).

U.S. District Court for the Northern District of Illinois, Eastern Division, Consolidated amended class action complaint, *In re TikTok, Inc., Consumer Privacy Litigation*, Case 1:20-cv-04699, MDL No. 2948, https://www.documentcloud.org/documents/20492025-amended-complaint-tiktok-consumer-privacy-litigation (December 18, 2020).

[116] Bobby Allyn, "TikTok to pay $92 million to settle class-action suit over 'theft' of personal data," National Public Radio, https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data (February 25, 2021).

Megan Sauer, "Some TikTok users are receiving $167 checks over data privacy violations—and Google and Snapchat could be next," CNBC, https://www.cnbc.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html (October 28, 2022).

U.S. District Court for the Northern District of Illinois, Eastern Division, Plaintiffs' motion for preliminary approval of class action settlement, *In re TikTok, Inc., Consumer Privacy Litigation*, Case 1:20-cv-04699, MDL No. 2948, https://s3.documentcloud.org/documents/20491862/plaintiffs-motion-for-preliminary-approval-of-class-action-settlement.pdf (February 25, 2021).

[117] Megan McCluskey, "TikTok has started collecting your 'faceprints' and 'voiceprints.' Here's what it could do with them," *TIME*, https://time.com/6071773/tiktok-faceprints-voiceprints-privacy (June 14, 2021).

[118] Office of the Attorney General, "Attorney General Bonta announces nationwide investigation into TikTok," California Department of Justice, Office of the Attorney General, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-nationwide-investigation-tiktok (March 2, 2022).

[119] Asuman Senol et al., "Leaky forms: A Study of email and password exfiltration before form submission," USENIX Security 2022, Boston, Massachusetts, August 10-12, 2022, https://homes.esat.kuleuven.be/%7Easenol/leaky-forms/leaky-forms-usenix-sec22.pdf (paper published March 13, 2022); follow-up study described at https://homes.esat.kuleuven.be/~asenol/leaky-forms/#advanced_matching (March 25, 2022).

129. In June 2022, *BuzzFeed News* reported on the contents of leaked audio recordings from more than eighty internal ByteDance meetings, including "14 statements from nine different TikTok employees indicating that engineers in China had access to US data between September 2021 and January 2022, at the very least." Nine additional statements from eight different employees indicated that US employees had to rely on their colleagues in China to tell them how US user data was flowing, since US staff was not authorized to independently access that data.[120]

130. In October 2022, *Forbes* reported that members of ByteDance's Internal Audit and Risk Control department had planned to use the TikTok app to monitor the physical location of specific American citizens who had never been employed by the company. Although a TikTok spokesperson claimed that the company only extrapolates the approximate location data of users from their IP addresses in order to select content and ads to display, to ensure legal compliance and detect fraud, the Internal Audit team accessed that information in order to surveil individual users.[121] In December 2022, TikTok CEO Shou Zi Chew admitted that employees in both the US and China accessed IP addresses and other personal data of a number of US users and journalists at *Buzzfeed News* and *Financial Times* (including the author of the report cited in the previous paragraph), in an attempt to ferret out the source of an embarrassing leak.[122]

131. In February 2023, the Office of the Privacy Commissioner of Canada and the Privacy Commissioners of Québec, Alberta, and British Columbia, announced a joint investigation into TikTok in order to determine whether the company's practices conform to Canadian law, especially as it pertains to the collection, use and disclosure of personal information, especially minors.[123]

132. In April 2023, the British Information Commissioner's Office fined TikTok £12.7 million for collecting the personal data of children under 13 without their parent's consent, in violation of the British General Data Protection Regulation. Information Commissioner John Edwards told the *Guardian*, "Our findings were that TikTok were not doing enough to prevent under-13s accessing their platform, they were not doing enough when they became aware of under-13s to

---

Lily Hay Newman, "US TikTok user data has been repeatedly accessed from China, leaked audio shows," *WIRED*, https://www.wired.com/story/leaky-forms-keyloggers-meta-tiktok-pixel-study (May 11, 2022).

[120] Emily Baker-White, "Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China," *BuzzFeed News*, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access (June 17,2022).

[121] Emily Baker-White, "TikTok parent ByteDance planned to use TikTok to monitor the physical location of specific American citizens," *Forbes*. https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=1dba4cfb6c2d (October 20, 2022).

[122] Mack DeGuerin, "TikTok owner admits employees accessed data of U.S. users and journalists," *Gizmodo*. https://gizmodo.com/tiktok-data-china-bytedance-1849924671 (December 22, 2022)

Reuters, "TikTok admits using its app to spy on reporters in effort to track leaks," *The Guardian*, https://www.theguardian.com/technology/2022/dec/22/tiktok-bytedance-workers-fired-data-access-journalists (December 23, 2022).

[123] Office of the Privacy Commissioner of Canada, "Commissioners launch joint investigation into TikTok," https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230223 (February 23, 2023).

get rid of them, and they were not doing enough to detect under-13s on there."[124] The ICO further charged that TikTok had failed to clearly describe the manner in which user data was collected and shared, and that it had failed to process users' personal data in accordance with British regulations.[125]

133. A May 2023 *New York Times* investigation found that TikTok users' personal information and documents (including driver's licenses, passports, and government identification cards) were frequently shared on Lark, the company's internal messaging and collaboration tool that was also readily accessible to workers at ByteDance in China. Reportedly, when one TikTok employee asked whether rules existed for handling user data in Lark, Will Farrell, the interim security officer of TikTok's US Data Security organization, stated, "No policy at this time."[126] (TikTok's US Data Security is now overseeing Project Texas, TikTok's migration of US data to Oracle servers in that state.)."[127] Although TikTok representatives asserted that the company was already taking steps to limit the size of Lark groups and to address the use of sensitive content, these findings nonetheless contradicted sworn statements by TikTok CEO Shou Zi Chew in his March 2023 testimony before Congress that the company already had "rigorous data access protocols."[128]

134. Also in May 2023, Forbes revealed that TikTok had been storing sensitive financial information—including Social Security and tax identification numbers—of its biggest content creators on Chinese servers,[129] contradicting TikTok CEO Shou Zi Chew's Congressional testimony that "American data has always been stored in Virginia and Singapore."[130]

135. In September 2023, Ireland's Data Protection Commissioner (DPC) fined TikTok €345 million for failure to adhere to the country's privacy laws pertaining to the processing of children's data. Relevant instances included TikTok's default practice of setting to "public" all

---

[124] Alex Hern and Aletha Adu, "TikTok fined £12.7m for illegally processing children's data." *The Guardian*. https://www.theguardian.com/technology/2023/apr/04/tiktok-fined-uk-data-protection-law-breaches (April 4, 2023).

[125] U.K. Information Commissioner's Office, "ICO fines TikTok £12.7 million for misusing children's data," https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data (April 4, 2023).

[126] Sapna Maheshwari and Ryan Mac, "Driver's licenses, addresses, photos: Inside how TikTok shares user data," *New York Times*, https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html (May 24, 2023).

[127] Sapna Maheshwari and Ryan Mac, "Driver's licenses, addresses, photos: Inside how TikTok shares user data," *New York Times*, https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html (May 24, 2023).

[128] U.S. House of Representatives, Committee on Energy and Commerce, "TikTok: How Congress can safeguard American Data Privacy and protect children from online harms," Transcript of hearing held March 23, 2023, U.S. Government Publishing Office, https://www.congress.gov/118/chrg/CHRG-118hhrg53839/CHRG-118hhrg53839.pdf (March 23, 2023).

[129] Alexandra Levine, "TikTok creators' sensitive financial information stored in China," *Forbes*, https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china (May 30, 2023).

[130] U.S. House of Representatives, Committee on Energy and Commerce, "TikTok: How Congress can safeguard American data privacy and protect children from online harms," Transcript of hearing held March 23, 2023, U.S. Government Publishing Office, https://www.congress.gov/118/chrg/CHRG-118hhrg53839/CHRG-118hhrg53839.pdf (March 23, 2023).

accounts for users under 16 years of age, and the company's failure to verify whether adults using the "family pairing" feature were actually the parent or legal guardian of children to whom they wished to be paired; this allowed unknown adults to exchange direct messages with children.[131] TikTok protested the decision, arguing that the DPC's criticisms had been addressed long before the investigation commenced, including making all new and existing accounts for 13-15-year-old users private by default, and creating an age-appropriate version of TikTok's privacy policy for young users.[132]

136. A December 2023 investigation by the *Sydney Morning Herald* found that TikTok's tracking pixels existed on some of Australia's most popular websites, and that user email addresses, mobile phone numbers and browsing histories were being collected by TikTok even before users were given the opportunity to consent to collection of personal data, in violation of Australia's Privacy Act 1988. Eighteen months after the Radboud University study cited above, the *Sydney Morning Herald* corroborated its findings regarding nonconsensual data collection: "TikTok uses a tool called 'automatic advanced matching' that sees when a user enters text into a form field or a search box, and if it looks like an email address or phone number, it scrapes that data. Following publication of the *Sydney Morning Herald* report, the TikTok Pixel was removed from a number of Australian websites and apps, including Vodafone, mental health apps Headspace and Beyond Blue, Western Sydney University, the Sydney Opera House, the Tourism Boards of Tasmania, Queensland and the Northern Territory, and numerous other organizations.[133]

137. In December 2023, the Australian Information Commissioner commenced an investigation into TikTok's handling of users' personal data, and into claims that it has accumulated data without consent from individuals who never installed the app by means of the TikTok Pixel. The Commissioner expressed concern that the sort of tracking pixels used by TikTok are "harmful, invasive and corrosive of online privacy," and urged reform of Australia's Privacy Act.[134]

---

[131] Irish Data Protection Commission, "Irish Data Protection Commission announces €345 million fine of TikTok," https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok (September 15, 2023).

Alexandra Levine, "TikTok hit with $370M fine in Europe over children's privacy missteps," *Forbes*, https://www.forbes.com/sites/alexandralevine/2023/09/14/tiktok-fine-europe-children-data-privacy-security (September 15, 2023).

[132] Elaine Fox, "Response to the Data Protection Commission's Decision," TikTok, https://newsroom.tiktok.com/en-ie/response-to-the-data-protection-commission (September 27, 2023).

[133] Sumeyya Ilanbey and David Swan, "Australian companies dump TikTok tracking tool amid privacy concerns," *Sydney Morning Herald*, https://www.smh.com.au/business/companies/australian-companies-dump-tiktok-tracking-tool-amid-privacy-concerns-20240110-p5ewc0.html (January 15, 2024).

[134] ABC News Australia, "Claims TikTok siphons personal data of non-users without consent examined by Australian Information Commissioner," ABC News Australia, https://www.abc.net.au/news/2023-12-28/tiktok-personal-information-data-scraping-australian-authorities/103271042 (December 28, 2023).

Australian Information Commissioner, "Statement on TikTok preliminary inquiries," https://www.oaic.gov.au/news/media-centre/statement-on-tiktok-preliminary-inquiries (May 29, 2024).

138. In March 2024, CNN reported that the FTC is investigating TikTok for continued violations of COPPA and for violating FTC prohibitions against "unfair or deceptive" business practices through its denial that user information could be accessed by persons in China.[135]

139. An April 2024 *Forbes* investigation found that sensitive and competitive information from TikTok advertisers, including Amazon.com, Disney and the *New York Times*, was made available to both TikTok and ByteDance staff. That information included financial agreements, tax information, creative assets, and information on the manner in which TikTok customers were targeting their own customers, all stored in an internal platform called "Make More Money" (aka "3M") shared by ByteDance and TikTok. According to the report, TikTok staff used advertisers' information to persuade them to match or exceed their competitors' outlay for TikTok ads. As one former employee recalled, "It was common practice for employees to request access to data structures or dashboards without providing a rationale, and it would be granted."[136]

140. In August 2024, the US Department of Justice and Federal Trade Commission sued ByteDance for violating the COPPA. The above-cited suit against TikTok's predecessor, Musical.ly, required the company to take specific measures to comply with COPPA. The current suit alleges that "from 2019 to the present, TikTok knowingly permitted children to create regular TikTok accounts and to create, view, and share short-form videos and messages with adults and others on the regular TikTok platform." Personal information of children was allegedly collected and retained without parental consent, including information from accounts created in "Kids Mode," a version of the app created for pre-teens; and parental requests to delete their children's accounts and personal information were often disregarded.[137]

141. These examples of TikTok's privacy violations demonstrate additional reasons why TikTok's collection of non-TikTok user data should be concerning to such non-TikTok users.

7.2. The Chinese Government Routinely Engages in Online Espionage Against the US and Its Allies

142. The threat posed by Chinese cyberespionage has increased over the years. Chinese cyberespionage activities include both intrusions into computer systems and data scraping for surveillance purposes. Thus, the Chinese government's connection with TikTok causes further privacy concerns, especially for Non-TikTok users.

---

[135] Josh Sisco, "TikTok's troubles just got worse: The FTC could sue them, too," *Politico*, https://www.politico.com/news/2024/03/26/biden-administration-tiktok-data-practices-00149139 (March 26, 2024).

Brian Fung, "FTC investigating TikTok over privacy and security," *CNN Business*, https://www.cnn.com/2024/03/26/tech/ftc-tiktok-probe-privacy-and-security/index.html (March 26, 2024).

[136] Alexandra Levine, "TikTok mishandled the data of hundreds of top American advertisers," *Forbes*, https://www.forbes.com/sites/alexandralevine/2024/04/17/tiktok-mishandled-advertisers-data-bytedance-china (April 17, 2024).

[137] U.S. Department of Justice, "Justice Department sues TikTok and parent company ByteDance for widespread violations of children's privacy laws," https://www.justice.gov/opa/pr/justice-department-sues-tiktok-and-parent-company-bytedance-widespread-violations-childrens (August 2, 2024).

143. The National People's Congress's Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China, published in March 2016, identifies big data as a fundamental strategic resource, the first time that data was incorporated into China's national strategic plan.[138]

144. In its 2022 "Annual Threat Assessment of the US Intelligence Community," the Office of the Director of National Intelligence wrote: "We assess that China presents the broadest, most active, and persistent cyber espionage threat to US Government. ... Beijing conducts cyber intrusions that affect US and non-US citizens beyond its borders—such as hacking journalists—to counter perceived threats to the CCP and tailor influence efforts. China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations. and private sector networks."[139]

145. In its 2023 "Annual Threat Assessment of the US Intelligence Community," the Office of the Director of National Intelligence reiterated its warning: "China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the US homeland, suppression of the free flow of information in cyberspace—such as US web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally."[140]

146. The threat has not subsided; rather, it has increased, and now encompasses the field of artificial intelligence. In its 2024 "Annual Threat Assessment of the US Intelligence Community," the Office of the Director of National Intelligence wrote: "China will continue to expand its global intelligence posture to advance the CCP's ambitions, challenge US national security and global influence, quell perceived regime threats worldwide, and steal trade secrets and IP to bolster China's indigenous S&T sectors. Officials of the PRC intelligence services will try to exploit the ubiquitous technical surveillance environment in China and expand their use of monitoring, data collection, and advanced analytic capabilities against political security targets beyond China's borders. China is rapidly expanding and improving its AI and big data analytics capabilities for intelligence operations."[141]

147. The list of alleged state-sponsored cyberespionage campaigns by the People's Republic of China against its perceived adversaries and supposed allies is a long one.

---

[138] Lotus Ruan, "When the winner takes it all: Big data in China and the battle for privacy," Australian Strategic Policy Institute, https://www.aspi.org.au/report/big-data-china-and-battle-privacy (June 22, 2018), citing to National People's Congress, "Outline of the 13th Five-Year Plan for the national economic and social development of the People's Republic of China," http://www.china.com.cn/lianghui/news/2016-03/17/content_38053101_8.htm (March 2016).

[139] Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (February 7, 2022).

[140] Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (February 6, 2023).

[141] Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (February 5, 2024).

148. In late 2009, hackers from the People's Republic of China exploited an intercept system that Google had incorporated into Gmail in order to comply with US government surveillance requests. Malware installed on Google's systems communicated with a server configured to receive data exfiltrated from Google and at least thirty-three other organizations. According to Google, the hackers sought access to the Gmail accounts of human rights activists focused on the PRC. Further investigation revealed that the attack, dubbed "Aurora," was a state-sponsored counterespionage operation.[142]

149. As previously noted, a 2017 cyberattack against the consumer credit reporting agency Equifax led to the theft of personally identifiable information of nearly half of all US citizens. Exploitation of a vulnerability in Equifax's dispute resolution website enabled hackers to harvest addresses, birth dates, Social Security numbers, and other data on 147.9 million persons. In 2020, the US Department of Justice indicted four Chinese nationals for spearheading the attack.[143]

150. Between 2014 and 2018, an extended breach of Marriott's Starwood guest reservation database exposed the personal identifying information of nearly half a billion persons. Hackers exfiltrated guests' names, addresses, phone numbers, email addresses, passport numbers, birth dates, gender, loyalty program and reservation information, and credit card payment information. Private investigators working for Marriott found tools, techniques and procedures used in previous attacks by Chinese hackers.[144]

151. In 2014, hackers targeted the Office of Personnel Management's security clearance records and made off with personal information on over 22 million individuals, including 5.6 million sets of fingerprints.[145] US officials attributed the theft to Chinese state-sponsored actors.[146] In August

---

[142] Kim Zetter, "Google hackers targeted source code of more than 30 companies," *Wired*, https://www.wired.com/2010/01/google-hack-attack (January 13, 2010).

Mathew J. Schwartz, "Google Aurora hack was Chinese counterespionage operation," *Dark Reading*, https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation (May 21, 2013).

[143] U.S. Federal Bureau of Investigation, "Chinese military hackers charged in Equifax breach," https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020 (February 10, 2020).

Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" *CSO Magazine*, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (February 12, 2020).

[144] Sasha Gressin, "The Marriott data breach," *Consumer Advice*, U.S. Federal Trade Commission, https://consumer.ftc.gov/consumer-alerts/2018/12/marriott-data-breach (December 4, 2018).

Christopher Bing, "Clues in Marriott hack implicate China - sources," Reuters, https://www.reuters.com/article/world/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504R/ (December 6, 2018).

[145] Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say (July 9, 2015).

David E. Sanger, "Hackers took fingerprints of 5.6 million U.S. workers, government says," *New York Times*, https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html (September 23, 2015).

2017, a Chinese national was arrested for allegedly using "Sakula," an unusual variety of malware that was deployed in the OPM attack, and in breaches of three other organizations.[147]

152. In January 2015, health insurance provider Anthem Blue Cross discovered that hackers had stolen personal identifying information of over 78 million American citizens. Four years later, the US Department of Justice indicted Chinese national Fujie Wang and others for the attack on Anthem and on systems of three other unnamed organizations involved in the technology, basic materials production, and telecommunications sectors.[148]

153. In July 2020, two Chinese citizens were indicted for engaging in a ten-year hacking campaign against hundreds of computer systems in the US, Australia, Belgium, Germany, Hong Kong, Japan, Lithuania, the Netherlands, Spain, South Korea, Sweden, and the United Kingdom. Targeted industries included high tech manufacturing; medical device, civil, and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. It was also alleged that the defendants probed for vulnerabilities in the systems of companies developing COVID-19 vaccines, tests, and treatments.[149]

154. In fall 2020, the National Security Agency discovered that Chinese military personnel had infiltrated and gained deep, persistent access into Japan's classified defense networks.[150]

155. In September 2020, federal indictments were handed down against seven residents of the People's' Republic of China for breaking into over 100 computer systems in the United States, Australia, Brazil, Chile, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Singapore, South Korea, Taiwan, Thailand, and Vietnam. The defendants also allegedly compromised government computer networks in the U.K., India and Vietnam.[151]

---

[146] Dominic Rush, "OPM hack: China blamed for massive breach of US government data," *The Guardian*, https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances (June 5, 2015).

[147] Devlin Barrett, "Chinese national arrested for allegedly using malware linked to OPM hack," *Washington Post*, https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html (August 24, 2017).

[148] Charles Riley, "Insurance giant Anthem hit by massive data breach," *CNN Business*, https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security (February 6, 2015).

U.S. Department of Justice, "Member of sophisticated China-based hacking group indicted for series of computer intrusions, including 2015 data breach of health insurer Anthem Inc. affecting over 78 million people," https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including (May 9, 2019).

[149] U.S. Department of Justice, "Two Chinese hackers working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research," https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (July 21, 2020).

[150] Ellen Nakashima, "China hacked Japan's sensitive defense networks, officials say," *Washington Post*, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon (August 8, 2023).

[151] U.S. Department of Justice, "Seven international cyber defendants, including "Apt41" actors, charged in connection with computer intrusion campaigns against more than 100 victims globally,"

156. A 2021 *Washington Post* review of Chinese documents found that the country was increasingly casting its surveillance dragnets beyond its borders, deploying its "public opinion analysis software" to collect data on foreign sources, including mining Western social media. Bids have been solicited to create a database of foreign journalists and academics; to analyze discussions of Hong Kong and Taiwan; and to monitor content produced by China's Muslim Uyghur population. Facebook and Twitter posts are scraped and stored on Chinese servers for later analysis. Trends involving sensitive information are reported to the Chinese censorship apparatus; whereas most alarms were sounded about domestic Chinese social media, since mid-2019, foreign social media is also monitored, with the goal of guiding and intervening in public opinion about China worldwide.[152]

157. In July 2021, four Chinese nationals—including three officers in the Hainan State Security Department—were indicted for a campaign to penetrate computer networks of dozens of entities located in the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland and the United Kingdom. Trade secrets and confidential business information were appropriated from government and educational entities and from organizations in the aviation, defense, health care, pharmaceuticals, and maritime industries. Stolen assets included technologies for submersible craft and autonomous vehicles, chemical formulas and genetic sequencing, and data from infectious disease research.[153]

158. In early 2023, China-based threat actor "Operation Soft Cell" launched cyberattacks against telecommunications providers in the Middle East. The initial attack involved infiltrating Microsoft Exchange servers, deploying web shells for command execution, then engaging in reconnaissance, theft of credentials, lateral movement, and data exfiltration.[154]

159. In March 2023, Chinese hacking group "Sharp Panda" used spear-phishing and vulnerabilities in Microsoft products and systems to attack target government agencies in Vietnam, Thailand and Indonesia.[155]

160. In March 2023, cybersecurity researchers in Slovakia identified an exploit used by China's "Mustang Panda" group to attack political organizations in Taiwan and Ukraine.[156]

---

https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer (September 16, 2020).

[152] Cate Cadell, "China harvests masses of data on Western targets, documents show," *Washington Post*, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html (December 31, 2021).

[153] U.S. Department of Justice, "Four Chinese Nationals working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including infectious disease research," https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion (July 19, 2021).

[154] Aleksandar Milenkoski et al., "Operation Tainted Love: Chinese APTs target telcos in new attacks," Sentinel Labs, https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks (March 23, 2023)

[155] Check Point Research, "Pandas with a soul: Chinese espionage attacks against Southeast Asian government entities," https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities (March 7, 2023).

161. In March 2023, the Chinese hacker group "Tick" attacked an East Asian data loss prevention company that contracts with military and government agencies. The attackers invaded the company's internal update servers in order to embed malware, and ultimately executed malware on the computers of its customers.[157]

162. Between November 2022 and April 2023, Chinese hackers used previously unseen plugins from a malicious bot framework to attack African telecommunications providers, with the primary goal of information-gathering.[158]

163. In April 2023, a PRC-based employee of a US telecommunications company was federally indicted for his efforts to disrupt videoconferences organized by a Chinese-American pro-democracy activist. The employee identified accounts associated with the dissident, caused his videoconferences to be hosted on a server known for lags in response time, terminated his meetings prematurely, and sought to block all accounts associated with the dissident. During a 2019 conference commemorating the Tiananmen Square Massacre, the employee and his co-conspirators entered the videoconference, played loud music, screamed, and threatened the pro-democracy participants.[159]

164. In May 2023, Belgium accused Chinese hackers of engaging in a phishing attack against parliamentarian Samuel Cogolati, following his authorship of a resolution warning against "crimes against humanity" against Uyghur Muslims in Xinjiang Province.[160]

165. In May 2023, Chinese hackers attacked government ministries and organizations in Kenya, including the office of the president of Kenya.[161]

166. In July 2023, Chinese hackers inserted ShadowPad malware into a Pakistani government app, and also targeted a state bank and telecommunications firm.[162]

---

[156] Alexandre Côté Cyr, "MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT," *WeLiveSecurity*, ESET, https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt (March 2, 2023).

[157] Facundo Muñoz, "The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia," *WeLiveSecurity*, ESET, https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia (March 14, 2023).

[158] Ravie Lakshmanan, "Daggerfly cyberattack campaign hits African telecom services providers," *The Hacker News*, https://thehackernews.com/2023/04/daggerfly-cyberattack-campaign-hits.html (April 20, 2023).

[159] U.S. Department of Justice, "40 officers of China's National Police charged in transnational repression schemes targeting U.S. residents," https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us (April 17, 2023).

[160] Yuan Yang, "Belgium's cyber security agency links China to spear phishing attack on MP," *Financial Times*, https://www.ft.com/content/5c32261c-b1a6-488e-9002-0ca9e0c8ff1b (March 1, 2023).

[161] Aaron Ross, James Pearson and Christopher Bing, "Chinese hackers attacked Kenyan government as debt strains grew," Reuters, https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24 (May 24, 2023).

[162] Ravie Lakshmanan, "Pakistani entities targeted in sophisticated attack deploying ShadowPad malware," *The Hacker News*, https://thehackernews.com/2023/07/pakistani-entities-targeted-in.html (July 18, 2023).

167. In July 2023, US officials disclosed that Chinese hackers had infiltrated the email accounts of Commerce Secretary Gina Raimondo and other State and Commerce Department officials in the leadup to Secretary of State Antony Blinken's trip to Beijing.[163] Further investigation revealed that 60,000 emails had been stolen.[164]

168. In July 2023, Microsoft announced that it had thwarted Chinese cyberattacks targeting western European governments. The attacks had commenced two months prior, and enabled unauthorized access to email accounts of twenty-five organizations and a number of individual consumers. Microsoft attributed the campaign to Storm-0558, a China-based, state-sponsored intelligence-gathering group that specializes in espionage, data theft, and credential access to systems of European government agencies.[165]

169. In August 2023, Microsoft announced that a China-based nation-state group known as Flax Typhoon had exfiltrated data from and established covert proxy networks within the computer systems of several Taiwanese organizations.[166]

170. In August 2023, Chinese hackers infiltrated Nebraska email accounts of Congressman Don Bacon, a member of the House Armed Services Committee.[167]

171. In September 2023, Microsoft reported escalating Chinese cyber operations in the South China Sea, and against the defense industry and critical infrastructure in the US.[168]

172. In September 2023, US and Japanese officials announced that Chinese hackers had modified router firmware in order to target both government and private industry.[169]

---

[163] Julian E. Barnes and Edward Wong, "Chinese hackers targeted Commerce Secretary and other U.S. Officials," *New York Times*, https://www.nytimes.com/2023/07/12/us/politics/china-state-department-emails-microsoft-hack.html (July 12, 2023).

[164] Karoun Demirjian, "Chinese hackers stole 60,000 State Dept. emails in breach reported in July," *New York Times*, https://www.nytimes.com/2023/09/27/us/politics/chinese-hackers-state-department.html (September 27, 2023).

[165] Ravie Lakshmanan, "Microsoft thwarts Chinese cyber attack targeting western European governments," *The Hacker News*, https://thehackernews.com/2023/07/microsoft-thwarts-chinese-cyber-attack.html (July 12, 2023).

Microsoft Security Response Center, "Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email," *MSRC Blog*, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email (July 11, 2023).

[166] Microsoft Threat Intelligence, "Flax Typhoon using legitimate software to quietly access Taiwanese organizations," *Microsoft Security Blog*, https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations (August 24, 2023).

[167] Joseph Menn, "Chinese spies who read State Dept. email also hacked GOP congressman," *Washington Post*, https://www.washingtonpost.com/technology/2023/08/14/microsoft-china-hack-congress (August 15, 2023).

[168] Clint Watts, "China, North Korea pursue new targets while honing cyber capabilities," *Microsoft on the Issues*, https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea (September 7, 2023)

[169] Cybersecurity and Infrastructure Security Agency, "People's Republic of China-linked cyber actors hide in router firmware," https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a (September 27, 2023).

173. In September 2023, reports surfaced that Chinese hackers had attacked the national power grid of an Asian country with Windows malware that enabled them to move laterally within the grid's computer network. The attack originated with a single compromised computer.[170]

174. In October 2023, news reports revealed that Chinese hackers had been engaged in a phishing campaign against the Guyanese government since February of that year.[171]

175. In November 2023, Chinese hackers attacked more than two dozen Cambodian government networks, disguising themselves as cloud storage services in order to facilitate their exfiltration of data.[172]

176. From August to November 2023, Chinese hackers used phishing to embed malware into Philippine government computer systems, in order to spy on its activities.[173]

177. In November 2023, China-based phishing campaigns sought to gain access to government computer systems in Uzbekistan and the Republic of Korea.[174]

178. In December 2023, the US Department of Justice disrupted a botnet consisting of hundreds of malware-infected small and home office routers that had been highjacked by China-based hackers in order to conceal the Chinese origins of an intelligence-gathering campaign against critical infrastructure in the US.[175]

Dan Goodin, "Backdoored firmware lets China state hackers control routers with "magic packets"," *Ars Technica*, https://arstechnica.com/security/2023/09/china-state-hackers-are-camping-out-in-cisco-routers-us-and-japan-warn (September 27, 2023).

[170] Brandon Vigliarolo, "China caught—again—with its malware in another nation's power grid," *The Register*, https://www.theregister.com/2023/09/12/china_malware_grid (September 12, 2023).

Ravie Lakshmanan, "Chinese Redfly group compromised a nation's critical grid in 6-month ShadowPad campaign," *The Hacker News*, https://thehackernews.com/2023/09/chinese-redfly-group-compromised.html (September 12, 2023).

[171] Ravie Lakshmanan, "Guyana governmental entity hit by DinodasRAT in cyber espionage attack," *The Hacker News,* https://thehackernews.com/2023/10/guyana-governmental-entity-hit-by.html (October 5, 2023).

[172] Ravie Lakshmanan, "Chinese hackers launch covert espionage attacks on 24 Cambodian organizations," *The Hacker News*, https://thehackernews.com/2023/11/chinese-hackers-launch-covert-espionage.html (November 13, 2023).

Unit 42, "Chinese APT targeting Cambodian government," Palo Alto Networks, https://unit42.paloaltonetworks.com/chinese-apt-linked-to-cambodia-government-attacks (November 7, 2023).

[173] Ravie Lakshmanan, "Mustang Panda hackers targets Philippines government amid South China Sea tensions," *The Hacker News*, https://thehackernews.com/2023/11/mustang-panda-hackers-targets.html (November 21, 2023).

[174] Ravie Lakshmanan, "Chinese hackers using SugarGh0st RAT to target South Korea and Uzbekistan," *The Hacker News*, https://thehackernews.com/2023/12/chinese-hackers-using-sugargh0st-rat-to.html (December 1, 2023).

[175] U.S. Department of Justice, "U.S. government disrupts botnet People's Republic of China used to conceal hacking of critical infrastructure," https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical (January 31, 2024).

179. In February 2024, an anonymous leak exposed 190 megabytes of data from Chinese cybersecurity firm I-Soon, showing that it had been engaged in espionage against the Indian, Indonesian, and Taiwanese governments; NATO, the UK foreign office, and citizens of Xinjiang Province.[176]

180. In February 2024, the Dutch defense ministry accused Chinese spies of placing malware in its military networks the previous year.[177]

181. In February 2024, ChatGPT developer OpenAI reported that it had terminated the accounts of malicious Chinese actors known as "Charcoal Typhoon" and "Salmon Typhoon." "Charcoal Typhoon" used OpenAI services to "research various companies and cybersecurity tools, debug code and generate scripts, and create content likely for use in phishing campaigns." "Salmon Typhoon" used OpenAI services to "translate technical papers, retrieve publicly available information on multiple intelligence agencies and regional threat actors, assist with coding, and research common ways processes could be hidden on a system."[178]

182. In February 2024, the US National Security Agency, the FBI, Transportation Security Administration, and the Cybersecurity and Infrastructure Security Agency (CISA) announced that a group nicknamed "Volt Typhoon" had infiltrated computer systems of numerous organizations involved in aviation, rail, mass transit, highway, maritime, pipeline, water, and sewage treatment.[179] In 2023, the *Washington Post* had reported that the Volt Typhoon group had infiltrated or attempted to infiltrate computer systems of a Hawaiian water utility, an oil and gas pipeline, the independent Texas power grid, and telecommunications firms in Guam.[180]According to CISA, rather than deploying malware, Volt Typhoon uses a technique

---

[176] Amy Hawkins, "Huge cybersecurity leak lifts lid on world of China's hackers for hire," *The Guardian*, https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire (February 23, 2024).

Frank Bajak and Dake Kang, "Leaked hacking files show Chinese spying on citizens and foreigners alike," *PBS News*, https://www.pbs.org/newshour/world/leaked-hacking-files-show-chinese-spying-on-citizens-and-foreigners-alike (February 21, 2024).

[177] James Pearson and Anthony Deutsch, "Chinese spies hacked Dutch defence network last year—intelligence agencies," Reuters, https://www.reuters.com/technology/cybersecurity/china-cyber-spies-hacked-computers-dutch-defence-ministry-report-2024-02-06 (February 6, 2024).

[178] Open AI, "Disrupting malicious uses of AI by state-affiliated threat actors," https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors (February 14, 2024).

[179] U.S. Cybersecurity and Infrastructure Security Agency, "PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (February 7, 2024).

The Guardian, "Chinese hackers infiltrated plane, train and water systems for five years, US says," *The Guardia*n, https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure (February 8, 2024).

[180] Ellen Nakashima and Joseph Menn, "China's cyber army is invading critical U.S. services," *Washington Post*, https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict (December 11, 2023).

Joseph Menn, "U.S. says Chinese hackers breached gear in Guam, key to Pacific defense," *Washington Post*, https://www.washingtonpost.com/technology/2023/05/24/china-hack-guam-taiwan.

called "living off the land" to evade detection by making use of built-in network administration tools and processes to mimic the behavior of authorized users. PowerShell commands are deployed in order to obtain valid user login credentials; the Windows Management Instrumentation command line is used to collect information about local drives; Impacket redirects output to the victim system's internal files.[181]

183. On March 25, 2024, the US Department of Justice indicted seven Chinese citizens—allegedly part of the "APT31 Group"—on charges of conspiracy to commit computer intrusions and wire fraud, stemming from a fourteen-year campaign of targeted hacking of "US and foreign critics, businesses, and political officials in furtherance of the PRC's economic espionage and foreign intelligence objectives."[182] The indictment alleges that the defendants targeted "individuals at the White House; the Departments of Justice, Commerce, Treasury and State; members of Congress, including both Democratic and Republican US Senators from more than ten states; government officials in the Eastern District of New York; and the spouses of a high-ranking Department of Justice official, high-ranking White House officials and multiple United States Senators," as well as numerous "political strategists and commentators and political and special interest advocates, and government contractors." The indictment further alleges that in 2021, the defendants targeted more than 400 email accounts of individuals associated with the EU's Inter-Parliamentary Alliance on China, a group founded the previous year with the purpose of countering "the threats posed by the Chinese Communist Party to the international order and democratic principles."[183] Targets included members of the Italian parliament, the head of Belgium's Foreign Affairs Committee, and the former Prime Minister of Belgium.[184]

184. Institutional victims named in the indictment include: seven IT managed service providers in New York, California, Massachusetts, Colorado, Idaho and overseas; a financial company in California; a nuclear power engineering company in California; an enterprise-resources planning company in California; a manufacturer of military flight simulators in Oklahoma; an aerospace and defense contractor in Tennessee; a professional support services company in Maryland; a manufacturer of software and computer services in California; a global provider of wireless technology in Illinois; a technology company in New York; an industrial control software

---

[181] U.S. Cybersecurity and Infrastructure Security Agency, "People's Republic of China state-sponsored cyber actor Living off the Land to evade detection," https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a (May 24, 2023).

Scott Jasper, "Chinese and Russian legitimate tool attacks mandate AI-enabled cyber defenses," The Cyber Edge, https://www.afcea.org/signal-media/cyber-edge/chinese-and-russian-legitimate-tool-attacks-mandate-ai-enabled-cyber (May 1, 2024).

[182] James Pearson, Raphael Satter and Christopher Bing, "US, UK accuse China of cyberespionage that hit millions of people," Reuters, https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25 (March 25, 2024).

[183] U.S. District Court, Eastern District of New York, Indictment, *U.S. v. Ni Gaobin et al.*, Case 24-CR-43, https://www.justice.gov/opa/media/1345141/dl?inline (January 30, 2024).

[184] Reuters, "Head of Belgian Foreign Affairs Committee says she was hacked by China," Reuters, https://www.reuters.com/world/europe/head-belgian-foreign-affairs-committee-says-she-was-hacked-by-china-2024-04-25 (April 25, 2024).

Antoaneta Roussi and Pieter Haeck, "Ex-Belgian PM Guy Verhofstadt was a victim of Chinese hacking ," *Politico*, https://www.politico.eu/article/ex-belgian-pm-guy-verhofstadt-was-a-victim-of-chinese-hacking (April 20, 2024).

company in California; an IT consulting company in California; an IT services and spatial processing company in Colorado; a multifactor authentication company; an American trade association; numerous information technology training and support companies; a leading provider of 5G network equipment; an IT solutions and 5G integration service company in Idaho; a telecommunications company in Illinois; a voice technology company in California; a manufacturing association in Washington, DC; a steel company; an apparel company in New York; an engineering company in California; an energy company in Texas; a finance company in New York; a multinational management consulting firm in Washington, DC; a financial ratings company in New York; an advertising agency in New York; a consulting company in Virginia; multiple global law firms; a law firm software provider; a machine-learning laboratory in Virginia; a university in California; numerous research hospitals and institutes in New York and Massachusetts; and an international nonprofit organization in Washington, DC. [185]

185. The same day the APT31 indictment was released, the US Department of the Treasury Office of Foreign Assets Control sanctioned Wuhan Xiaoruizhi Science and Technology Company, Ltd., and two of the employees named in the indictment for their participation in malicious cyber operations targeting US critical infrastructure on behalf of the Chinese government.[186]

186. Simultaneously, the UK Home Office and National Cyber Security Centre announced that between 2021 and 2022, the same group was very likely to have compromised the UK Electoral Commission, and had conducted reconnaissance activity against a number of UK parliamentarians who had been vocal in their criticisms of China's malign cyber activity.[187]

187. The New Zealand Government Communications Security Bureau also publicly disclosed that it had attributed a series of 2021 cyberattacks against the parliamentary counsel office and parliamentary service to the Chinese Ministry of State Security.[188]

---

[185] U.S. District Court, Eastern District of New York, Indictment, *U.S. v. Ni Gaobin et al.*, Case 24-CR-43, https://www.justice.gov/opa/media/1345141/dl?inline (January 30, 2024).

[186] U.S. Department of Justice, "Seven hackers associated with Chinese government charged with computer intrusions targeting perceived critics of China and U.S. businesses and politicians," https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived (March 25, 2024).

U.S. Department of the Treasury, "Treasury sanctions China-linked hackers for targeting U.S. critical infrastructure," https://home.treasury.gov/news/press-releases/jy2205 (March 25, 2024).

[187] Andrew Macaskill and James Pearson, "Britain says China hacked electoral watchdog, targeted lawmaker emails," Reuters, https://www.reuters.com/world/uk/uk-deputy-pm-set-address-lawmakers-chinese-cyber-security-threat-2024-03-24 (March 25, 2024).

U.K. National Cyber Security Centre, "UK calls out China state-affiliated actors for malicious cyber targeting of UK democratic institutions and parliamentarians (March 25, 2024).

U.K. Home Office, "UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity," https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity (March 25, 2024).

[188] Eva Corlett, "New Zealand parliament targeted in China-backed hack in 2021, spy agency says," *The Guardian*, https://www.theguardian.com/world/2024/mar/26/new-zealand-parliament-china-hack-2021-spy-agency-gcsb (March 25, 2024).

188. Canada's Communications Security Establishment stated that APT31 had also targeted Canada, but withheld details of the attacks.[189]

189. In April 2024, Microsoft reiterated its warning about Chinese threat actors and their sophisticated phishing and hacking campaigns in East Asia. The primary targets of "Gingham Typhoon" are the South Pacific islands; "Raspberry Typhoon" has targeted military entities in Indonesia, and attacked a Malaysian maritime system in the runup to a multilateral naval exercise the South China Sea; "Storm-0062" focuses on the US defense industrial base and critical infrastructure. Chinese influence operations in the region have used AI-generated or AI-enhanced content to stoke and amplify divisions within the region, including via the dissemination of deepfake audio clips of an independent candidate in Taiwan's presidential race.[190]

190. In June 2024, the government of Palau—one of the few countries that acknowledges Taiwan's status as an independent democracy—accused China of stealing more than 20,000 government documents in March 2024, after the country entered into a twenty-year economic and security agreement with the United States.[191]

191. In July 2024, Germany accused China of conducting a 2021 attack on the country's federal cartography agency, which conducts precision mapping of the country.[192]

192. In July 2024, the Australian Signals Directorate, the US Cybersecurity and Infrastructure Security Agency, and security divisions of Canada, the UK, New Zealand, Germany, South Korea, and Japan issued a joint advisory describing technical methods employed in attacks against Australian networks by the PRC state-sponsored group "APT40."[193]

193. In September 2024, security researchers reported that Chinese hackers had weaponized Visual Studio Code's embedded reverse shell feature to gain entry into target networks in an unnamed Southeast Asian government.[194]

---

[189] Ashley Burke, "Canada targeted by same Chinese hackers the U.S., U.K. accuse of cyberespionage that hit millions," CBC, https://www.cbc.ca/news/world/cyberespionage-china-hack-canada-targetted-1.7155482 (March 26, 2024).

[190] Microsoft Threat Intelligence, "Same targets, new playbooks: East Asia threat actors employ unique method," Microsoft, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf (April 2024).

[191] Jacob Judah, "Why a Pacific island is blaming China for a hack?" *New York Times*, https://www.nytimes.com/2024/06/02/world/asia/palau-taiwan-china-hack.html (June 2, 2024).

[192] Reuters, "Germany accuses China of conducting 2021 cyberattack on cartography agency," Reuters, https://www.reuters.com/world/germany-summons-chinese-ambassador-over-2021-cyberattack-cartography-agency-2024-07-31 (July 31, 2024).

[193] U.S. Cybersecurity and Infrastructure Security Agency, "People's Republic of China (PRC) Ministry of State Security APT40 tradecraft in action," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a (July 8, 2024).

[194] Ravie Lakshmanan, "Chinese hackers exploit Visual Studio code in Southeast Asian cyberattacks," *The Hacker News*, https://thehackernews.com/2024/09/chinese-hackers-exploit-visual-studio.html (September 9, 2024)/

194. It is understandable that some US citizens who are aware of the extent of China's espionage against the US and its allies, of the technical sophistication of its hacking campaigns, and of its efforts to undermine the security of its perceived adversaries, would seek to avoid engaging with any online platforms that originate in China, and that demand that users consent to the collection of vast amounts of personal information as the price of admission.

7.4 TikTok Is Legally Mandated to Provide Data to the Chinese Government If Ordered to Do So

195. China's National Intelligence Law, passed in 2017 and amended the following year, states that all Chinese citizens and private entities—including TikTok—"shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[195]

196. Given the US government's concern about Chinese government access to the personal online data of TikTok's 150 million US users, as well as information collected about non-TikTok users via apps built with the TikTok Pixel and Events API, in June 2022, TikTok embarked on a joint venture with Oracle, dubbed "Project Texas," to migrate all US user traffic to the Oracle Cloud Infrastructure.[196] Concern remains, however, that Chinese ByteDance executives could instruct their American colleagues to manipulate TikTok's "For You" video recommendation algorithm to push material sympathetic to the PRC, and to influence the American political process.[197]

197. In June 2023, former ByteDance employee Yintao Yu alleged in a court filing that in 2018, the Chinese Communist Party identified the locations and communications of protesters in Hong Kong by way of backdoor access to TikTok. Yu alleged that CCP officials possessed a "god credential" enabling them to bypass TikTok's ordinary privacy protections.[198]

198. It is understandable that some US citizens who are aware of China's legislation requiring cooperation with the country's intelligence services would seek to avoid engaging with any online platform that originates in China.

Tom Fakterman, "Chinese APT abuses VSCode to target government in Asia," Palo Alto Networks, https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage (September 6, 2024).

[195] China Law Translate, "PRC National Intelligence Law," https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017 (June 27, 2017).

Murray Scot Tanner, "Beijing's new National Intelligence Law: From defense to offense," *Lawfare*, https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense (July 20, 2017).

[196] TikTok, "Delivering on our US data governance," https://usds.tiktok.com/delivering-on-our-us-data-governance (January 24, 2023).

[197] Emily Baker-White, "Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China," *BuzzFeed News*, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access (June 17, 2022).

[198] Brian Fung, "There is now some public evidence that China viewed TikTok data," *CNN Business*, https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html (June 8, 2023).

7.5 TikTok Has Historically Stored US Data Overseas, and Sent Some US Data to Its Data Center in Singapore

199. There is a conflict between the TikTok's desire for data and non-TikTok users' desire for privacy. The desire for privacy conflicts with competing demands of the online advertising business model for maximization of data collection, which creates a strong incentive to overpromise and underdeliver on privacy.

200. [redacted]

7.6 Non-TikTok Users Have Reasons to Deliberately Attempt to Avoid Surveillance by TikTok

202. The history of TikTok security breaches, China's practice of surveilling its own citizens, and Chinese espionage against the US and other nations have led to growing concern on the part of both users and lawmakers regarding TikTok's collection and storage of data on US citizens, and the potential for that data to be appropriated on demand by the Chinese government. These issues raise additional privacy concerns concerning TikTok, especially as to non-TikTok users.

203. In October 2021, the Senate Committee on Commerce, Science and Transportation held a hearing on children's use of social media that included testimony by Michael Beckerman, Vice President and Head of Public Policy at TikTok. During that hearing, Beckerman assured legislators that "All US user data collected on the TikTok platform is stored on servers located in the US, with backup data stored on servers in Singapore," and that ByteDance has "no input into TikTok's operations."[203]

---

[199] Defendants' Amended Responses and Objections to Plaintiffs' Interrogatory Nos. 6 and 13.

[200] Id.

[201] *See* TIKTOK-BG-000439076 [redacted]

[202] See TIKTOK-BG-000168680.

[203] U.S. Senate, Committee on Commerce, Science and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security, "Subcommittee: Protecting Kids Online: Snapchat, TikTok, and YouTube," Transcript of hearing held October 26, 2021, https://www.govinfo.gov/content/pkg/CHRG-117shrg54901/pdf/CHRG-117shrg54901.pdf (October 26, 2021).

Rachel Lerman and Cristiano Lima-Strong, "TikTok, Snap, YouTube defend how they protect kids online in congressional hearing," *Washington Post*, https://www.washingtonpost.com/technology/2021/10/26/tiktok-snapchat-youtube-congress-hearing (October 26, 2021).

204. These assurances are misleading. Although TikTok executives have insisted that TikTok is a US entity quite separate from ByteDance, a 2021 CNBC report revealed that TikTok employees were required to participate in meetings with ByteDance executives and to be available to answer questions about TikTok from ByteDance employees, and that ByteDance employees had exclusive access to certain categories of user data, including data about US residents who searched for or interacted with content bearing specific terms or hashtags.[204] In 2022, the *Wall Street Journal* reported that senior TikTok algorithm engineers were based in China, and that ByteDance recruited people throughout China to work on TikTok features such as private messaging, live-streaming, and its marketplace functions.[205]

205. A November 2023 report by Amnesty International found that TikTok's "highly extractive business model fundamentally undermines human rights" via its algorithms, which "can infer our moods, ethnicities, sexual orientation, political opinions, and vulnerabilities." The surveillance-based business model "represents an intrusion into billions of people's private lives that can never be necessary or proportionate." Young TikTok users in particular experience interference with their "ability to shape their own identities within a private sphere," and to maintain privacy in their thoughts and opinions. TikTok's advertising systems discriminate between users, grouping users into various demographic and interest categories so that they might be targeted by advertisers. Inferences about a user's health status or sexuality, for example, impinge on users' right not to reveal their inner thoughts.[206]

206. Efforts to restrict or ban TikTok nationally have snowballed, with some attempts more successful than others. Donald Trump's 2020 executive order banning the app failed in the aftermath of a federal court order finding that insufficient proof of harm exists to justify violating American's First Amendment rights.[207] President Biden subsequently revoked the order, while establishing criteria for evaluating the risk of apps associated with foreign adversaries.[208]

---

[204] Salvador Rodriguez, "TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance," CNBC, https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html (June 25, 2021).

[205] Raffaele Huang, "TikTok's efforts to distance itself from Chinese parent stumble over talent," *Wall Street Journal*, https://www.wsj.com/articles/tiktoks-efforts-to-cut-ties-with-chinese-parent-stumble-over-talent-11671186110 (December 16, 2022).

[206] Amnesty International, 'I feel exposed': Caught in TikTok's surveillance web," Amnesty International Report POL 40/7349/2023, https://www.amnesty.org/en/documents/pol40/7349/2023/en (November 7, 2023).

[207] U.S. Office of the President, "Executive order on addressing the threat posed by TikTok," https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok (August 6, 2020).

U.S. District Court for the District of Columbia, Memorandum opinion, *TikTok v. Trump*, Case 1:20-cv-02658 (CJN), https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv2658-30 (September 27, 2020).

Drew Harwell, "TikTok and the U.S. government dig in for a legal war over potential ban," *Washington Post*, https://www.washingtonpost.com/technology/2024/04/25/tiktok-legal-battle-is-certain (April 25, 2024).

[208] Salvador Rodriguez, "TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance," CNBC, https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html (June 25, 2021).

207. In December 2022, President Joe Biden signed into law a bill banning the use of the TikTok app on devices used by the federal government's nearly four million employees.[209]

208. In June 2023, Senators Richard Blumenthal and Marsha Blackburn wrote to TikTok CEO Shou Zi Chew regarding reports in the New York Times[210] and Forbes[211] that the platform "allowed private data about American users to be stored and accessed in China, despite his repeated public assurances and Congressional testimony that TikTok data was kept in the United States."[212] In its response, TikTok distinguished between data provided by US users during registration and use of the app, and data provided by prominent content creators—that is, data that falls under a "limited exception"; whereas it stated the former is kept on servers in the US and Singapore, it did not specify where the latter data is kept, only that it is "excepted" from the policies that govern the storage of user data.[213]

209. In March 2024, Blumenthal and Blackburn wrote to the Director of National Intelligence urging declassification of information on TikTok and ByteDance so that American citizens can be better informed of the risk that TikTok's Chinese ownership poses to US national security.[214]

210. Congressional hearings, Blumenthal and Blackburn's efforts to publicize their grave concerns about TikTok, and the stream of media reports on TikTok's security lapses and on China's campaign of incursions into US computer networks and systems have yielded increased momentum within Congress for a complete nationwide ban on the TikTok app.[215]

---

[209] David Ingram, "Biden signs TikTok ban for government devices, setting up a chaotic 2023 for the app," NBC News, https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724 (December 30, 2022).

[210] Sapna Maheshwari and Ryan Mac, "Driver's licenses, addresses, photos: Inside how TikTok shares user data," *New York Time*s, https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html (May 24, 2023).

[211] Alexandra Levine, "TikTok creators' sensitive financial information stored in China," *Forbes*, https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china (May 30, 2023).

[212] Richard Blumenthal and Marsha Blackburn, Letter to Shou Zi Chew, Chief Executive Officer, TikTok, https://www.blackburn.senate.gov/services/files/76E769A8-3EDA-4BA0-989E-42D5F99E547D (June 6, 2023).

[213] TikTok, Letter to Senators Richard Blumenthal and Marsha Blackburn, https://www.blackburn.senate.gov/services/files/A4595D03-689A-43FF-ADBA-32C557DE3685 (June 16, 2023).

[214] Richard Blumenthal and Marsha Blackburn, Letter to Avril Haines, Director of National Intelligence, https://www.blumenthal.senate.gov/imo/media/doc/3212024odnitiktokdeclassification.pdf (March 21, 2024).

Sapna Maheshwari, "Senators say TikTok may have misled Congress on handling of U.S. user data," *New York Times*, https://www.nytimes.com/2023/06/07/technology/tiktok-congress-user-data.html (June 7, 2023).

[215] Scott Wong, Kate Santaliz and Liz Brown-Kaiser, "Momentum builds in Congress to crack down on TikTok," NBC News, https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998 (February 18, 2023).

Kevin Collier and Scott Wong, "White House backs bipartisan bill that could be used to ban TikTok," NBC News, https://www.nbcnews.com/tech/tech-news/restrict-act-bill-tiktok-rcna73682 (March 7, 2023) (RESTRICT Act).

Gavin Bade, "Lawmakers shift gears on TikTok ban," *Politico*, https://www.politico.com/news/2023/10/09/what-happened-to-the-tiktok-ban-00120434 (October 9, 2023). (Guard Act).

211. H.R. 7521, the Protecting Americans from Foreign Adversary Controlled Applications Act, was introduced by Rep. Mike Gallagher on March 5, 2024, and one week later was overwhelmingly passed by the House with a vote of 352–65.[216] After the bill was received in the Senate, it was modified to give more time for TikTok to sever itself from ByteDance, and incorporated into H.R. 815, an appropriations bill.[217]

212. In April 2024, POLITICO reported that Chinese embassy personnel were meeting with congressional staff in efforts to persuade them against forcing divestiture of TikTok from ByteDance, downplaying national security concerns, and arguing that the legislation "amounted to a forced data transfer of a Chinese company"—this in spite of TikTok's efforts to distance itself from its Chinese origins.[218]

213. In April 2024, President Biden signed H.R. 815 into law. The relevant section[219] gives TikTok 270 days to divest from its parent company ByteDance or risk being banned from app stores in the United States.[220] TikTok CEO Shou Zi Chew has declared that TikTok will challenge all such laws through the courts, and has made good on that promise. On September 16, 2024, the US Court of Appeals for the DC Circuit heard arguments in TikTok's lawsuit against the constitutionality of the law; a ruling has yet to be issued.[221]

214. State legislatures have separately been debating bans on the TikTok app as well. Although Montana became the first state to pass a ban in May 2023,[222] a federal court struck it down

---

[216] U.S. Congress, H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, https://www.congress.gov/bill/118th-congress/house-bill/7521 (March 13, 2024).

Rebecca Kern, "TikTok's biggest threat just passed the House," *Politico*, https://www.politico.com/news/2024/03/13/tiktok-ban-bill-house-passes-00146720 (March 13, 2024).

Scott Wong, Kate Santaliz and Liz Brown-Kaiser, "Momentum builds in Congress to crack down on TikTok," NBC News, https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998 (February 18, 2023).

[217] U.S. Congress, H.R.815 -- Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes https://www.congress.gov/bill/118th-congress/house-bill/815 (signed into law April 24, 2024).

[218] Hailey Fuchs, "Chinese diplomats are quietly meeting with Hill staffers about TikTok," *Politico*, https://www.politico.com/news/2024/04/17/china-lobbying-tiktok-congress-00152819 (April 17, 2024).

Madison Hall, "China just proved why Congress wants to ban TikTok," *Business Insider*, https://www.businessinsider.com/china-just-proved-why-congress-wants-to-ban-tiktok-2024-4 (April 17, 2024).

[219] Division H—Protecting Americans from Foreign Adversary Controlled Applications Act

[220] Brian Fung, "Biden just signed a potential TikTok ban into law. Here's what happens next," *CNN Business*, https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html (April 24, 2024).

Drew Harwell, "TikTok and the U.S. government dig in for a legal war over potential ban," *Washington Post*, https://www.washingtonpost.com/technology/2024/04/25/tiktok-legal-battle-is-certain (April 25, 2024).

[221] Alison Durkee, "TikTok ban heard today in court—Here's what to know," *Forbes*, https://www.forbes.com/sites/alisondurkee/2024/09/16/tiktok-ban-heard-today-in-court-heres-what-to-know (September 16, 2024).

[222] Brian Fung, "Montana lawmakers vote to completely ban TikTok in the state," CNN Business, https://www.cnn.com/2023/04/14/tech/montana-house-tiktok-ban/index.html (April 14, 2020).

shortly after its passage; opponents of the law argued that it would violate the First Amendment rights of TikTok users, and the court subsequently ruled that the law "oversteps state power" and that it was more focused on "China's ostensible role in TikTok" than on protecting Montana consumers.[223]

215. Approximately thirty-four states, as well as New York City, have banned the TikTok app from government devices.[224]

Samantha Delouya, "Montana governor bans TikTok," CNN Business, https://www.cnn.com/2023/05/17/tech/montana-governor-tiktok/index.html (May 18, 2023).

Montana 68th Legislature 2023, "An act banning TikTok in Montana," SB0419, https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf (effective January 1, 2024).

David Shepardson, "Virginia, other US states back Montana in TikTok ban -_court filing," Reuters, https://www.reuters.com/legal/virginia-other-us-states-back-montana-tiktok-ban-court-filing-2023-09-18 (September 18, 2023).

[223] Drew Harwell, "Montana ban on TikTok blocked, extending critics' losing streak," *Washington Post*, https://www.washingtonpost.com/technology/2023/11/30/tiktok-ban-montana-blocked (November 30, 2023).

[224] Aajene Robinson, "Alabama Gov. Kay Ivey bans TikTok on state devices," WBRC, https://www.wbrc.com/2022/12/14/alabama-gov-kay-ivey-bans-tiktok-state-devices (December 14, 2022) (Alabama); Iris Samuels, "Alaska bans the use of TikTok on state-owned devices," *Anchorage Daily News*, https://www.adn.com/politics/2023/01/06/alaska-bans-the-use-of-tiktok-on-state-owned-devices/ (January 6, 2023) (Alaska); FOX 10 Phoenix, "Arizona Gov. Hobbs bans TikTok on state devices," FOX 10 Phoenix, https://www.fox10phoenix.com/news/arizona-gov-hobbs-bans-tiktok-on-state-devices (April 5, 2023) (Arizona); Kelly Laco, "Sarah Huckabee Sanders bans TikTok on state devices in first move as Arkansas governor," FOX News, https://www.foxnews.com/politics/sarah-huckabee-sanders-bans-tiktok-state-devices-first-move-arkansas-governor (January 10, 2023) (Arkansas); Meredith Newman, "Delaware bans the use of TikTok on state devices due to cybersecurity concerns," *Delaware News Journal*, https://www.delawareonline.com/story/news/politics/2023/02/09/delaware-bans-tiktok-on-state-devices/69888579007 (February 9, 2023) (Delaware); Jeff Amy, "Georgia, NH latest states to ban TikTok from state computers," AP News, https://apnews.com/article/technology-georgia-8e62e34976ef070a9e24305248981684 (December 15, 2022) (Georgia, New Hampshire); Brad Little, "Gov. Little bans TikTok on state-issued devices," *East Idaho News*, https://www.eastidahonews.com/2022/12/gov-little-bans-tiktok-on-state-issued-devices (December 14, 2022) (Idaho); Associated Press, "TikTok blocked from Indiana state devices," WTHR, https://www.wthr.com/article/news/local/indiana-blocks-chinese-owned-app-tiktok-from-state-devices-social-media/531-7bb0ccc2-29b2-47bb-a1be-71aa836b03b3 (December 30, 2022) (Indiana); Liam Halawith, "Gov. Kim Reynolds bans TikTok on state-owned devices," *Daily Iowan*, https://dailyiowan.com/2022/12/14/governor-kim-reynolds-bans-tiktok-on-state-owned-devices (December 14, 2022) (Iowa); John Hanna, "Kansas' Democratic governor imposes TikTok ban," AP News, https://apnews.com/article/kansas-tik-tok-ban-explainer-83ef9bc3ff44d90e7b0f54bd8f5228cb (December 28, 2022) (Kansas); Divya Karthikeyan, "TikTok banned from Kentucky government devices," WKMS, https://www.wkms.org/government-politics/2023-01-16/tiktok-banned-from-kentucky-government-devices (January 16, 2023) (Kentucky); Associated Press, "Louisiana's secretary of state bans TikTok on devices issued by Department of State," FOX News, https://www.foxnews.com/us/louisianas-secretary-state-bans-tiktok-devices-issued-department-state (December 20, 2022) (Louisiana); Associated Press, "Maine is the latest state to ban TikTok for state workers," AP News, https://apnews.com/article/politics-maine-state-government-china-business-734ce1f1abde9c3b2a9c8172c6763d01 (January 19, 2023) (Maine); Olafimihan Oshin, "Hogan orders TikTok ban for Maryland government employees," *The Hill*, https://thehill.com/policy/technology/3764025-hogan-orders-tiktok-ban-for-maryland-government-employees (December 6, 2022) (Maryland); Michael Goldberg, "Mississippi governor bans TikTok from government devices," AP News, https://apnews.com/article/politics-mississippi-state-government-tate-reeves-business-b3658341702baf2a49ab0afbb618ee98 (January 11, 2023) (Mississippi); Mike Allen, "Nevada bans TikTok on government devices," KDRV, https://www.kdrv.com/news/national/nevada-bans-tiktok-on-government-devices/article_03e9903f-9fd7-553f-8ddb-9d6e82fec880.html (March 29, 2023) (Nevada); Stephen Neukam, "NJ

216. In February 2023, citing security concerns, the European Commission and Council of the European Union banned their 32,000 staff members from using TikTok on both work and personal devices with work apps installed on them.[225]

217. In March 2023, the Dutch government instructed its officials to uninstall apps from countries engaging in an "offensive cyber program" against it; these include China, Russia, North Korea and Japan.[226]

VIII. Conclusion

218. An expectation of privacy exists in America. This expectation of privacy extends to one's personal online data. TikTok's collection of vast amounts of data from non-TikTok users, who would have had no idea that TikTok was collecting their data from non-TikTok websites,

---

governor bans TikTok on state devices," *The Hill*, https://thehill.com/homenews/state-watch/3805699-nj-governor-bans-tiktok-on-state-devices/ (January 9, 2023) (New Jersey); WBTV, "N.C. Gov. Cooper signs executive order initiating ban of TikTok, WeChat from state devices," WBTV, https://www.wbtv.com/2023/01/12/nc-gov-roy-cooper-signs-executive-order-initiating-ban-tiktok-wechat-state-devices (January 12, 2023) (North Carolina); Julia Musto, "North Dakota governor bans TikTok app in executive branch agencies," *FOX Business*, https://www.foxbusiness.com/technology/north-dakota-governor-bans-tiktok-app-executive-agencies (December 14, 2022) (North Dakota); Lauren Sforza, "Ohio joins list of states banning TikTok on government electronic devices," *The Hill*, https://thehill.com/homenews/state-watch/3805512-ohio-joins-list-of-states-banning-tiktok-on-government-electronic-devices (January 9, 2023) (Ohio); Ryan Love, "Oklahoma Gov. Stitt bans TikTok on government devices," KJRH, https://www.kjrh.com/news/local-news/oklahoma-gov-stitt-bans-tiktok-on-government-devices (December 28, 2022) (Oklahoma); WYFF, "TikTok off-limits for South Carolina employees on state devices, governor says," WYFF, https://www.wyff4.com/article/tiktok-south-carolina-employees-state-devices/42157146 (December 5, 2022) (South Carolina); Stephen Groves, "South Dakota Gov. Noem bans TikTok from state-owned devices," AP News, https://apnews.com/article/south-dakota-bans-tiktok-from-state-devices-f7a95dd494dab9c410ff80c577c609dd (November 29, 2022) (South Dakota); NBCDFW, "Gov. Abbott bans TikTok on state-issued devices over cybersecurity concerns," NBC Dallas-Fort Worth, https://www.nbcdfw.com/news/local/texas-news/gov-abbott-bans-tiktok-on-state-issued-laptops-phones-and-other-devices/3143349 (December 7, 2022) (Texas); Olafimihan Oshin, "Utah governor orders TikTok ban for state government employees," *The Hill*, https://thehill.com/homenews/state-watch/3772150-utah-governor-orders-tiktok-ban-for-state-government-employees (December 12, 2022) (Utah); Fred Thys, "Vermont state government bans TikTok on its devices," *VT Digger*, https://vtdigger.org/2023/02/20/vermont-state-government-bans-tiktok-on-its-devices (February 20, 2023) (Vermont); Jared Gans, "Youngkin joins GOP governors in banning TikTok on state devices, wireless networks," *The Hill*, https://thehill.com/homenews/state-watch/3778557-youngkin-joins-gop-governors-in-banning-tiktok-on-state-devices-wireless-networks (December 16, 2022) (Virginia); Lawrence Andrea, "Gov. Tony Evers issues order banning TikTok on most state-issued devices," *Milwaukee Journal Sentinel*, https://www.jsonline.com/story/news/politics/2023/01/12/tony-evers-issues-order-banning-tiktok-on-some-state-issued-devices/69803482007 (January 12, 2023) (Wisconsin); Leo Wolfson, "Wyoming Gov. Mark Gordon bans TikTok on all state owned devices," *Cowboy State Daily*, https://cowboystatedaily.com/2022/12/15/wyoming-gov-mark-gordon-bans-tiktok-on-all-state-owned-devices (December 15, 2022) (Wyoming); Jonathan Franklin, "New York City officially bans TikTok on all government devices," National Public Radio, https://www.npr.org/2023/08/17/1194422613/new-york-city-bans-tiktok-government-devices (August 17, 2023) (New York City).

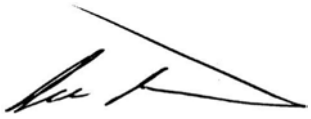
[225] Jamil Anderlini and Clothilde Goujard, "Brussels moves to ban Eurocrats from using TikTok," *Politico*, https://www.politico.eu/article/european-commission-to-staff-dont-use-tiktok (February 23, 2023).

[226] Pieter Haeck, "Beyond TikTok, Dutch tell government staff to uninstall Chinese, Russian apps," *Politico*, https://www.politico.eu/article/the-netherlands-china-russia-cyber-security-xi-jinping-vladimir-putin-recommends-officials-to-uninstall-apps (March 21, 2023).

violates this expectation of privacy. TikTok's privacy violations are all the more concerning, given that TikTok itself has both an affiliation with the Chinese government, and a history of US-based privacy violations.

219. This report sets forth my opinions based on the information currently available to me as of September 20, 2024. I reserve the right to amend or supplement this report based on additional information coming to my attention including, but not limited to, additional discovery, deposition testimony, and evidence presented at the trial of this case.

Respectfully submitted by,



/s/ Bruce Schneier

September 20, 2024

Expert Report of Bruce Schneier

September 20, 2024

Appendix I

Materials Considered

Public Exhibits

Paywalled material is marked with an asterisk, with full text appended at the end of this document.

ABC News Australia, "Claims TikTok siphons personal data of non-users without consent examined by Australian Information Commissioner," ABC News Australia, https://www.abc.net.au/news/2023-12-28/tiktok-personal-information-data-scraping-australian-authorities/103271042 (December 28, 2023).

Mark Ackerman, "Sales of public data to marketers can mean big $$ for governments," CBS Denver, https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments (August 26, 2013).

Mike Allen, "Nevada bans TikTok on government devices," KDRV, https://www.kdrv.com/news/national/nevada-bans-tiktok-on-government-devices/article_03e9903f-9fd7-553f-8ddb-9d6e82fec880.html (March 29, 2023).

Bobby Allyn, "Class-action lawsuit claims TikTok steals kids' data and sends it to China," National Public Radio, https://www.npr.org/2020/08/04/898836158/class-action-lawsuit-claims-tiktok-steals-kids-data-and-sends-it-to-china (August 4, 2020).

Bobby Allyn, "TikTok to pay $92 million to settle class-action suit over 'theft' of personal data," National Public Radio, https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data (February 25, 2021).

Alphabet, Inc., "Form 10-K," United States Securities and Exchange Commission, https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf?cache=5ae4398 (February 3, 2023).

Amnesty International, "Driven into darkness: How TikTok's 'For You' feed encourages self-harm and suicidal ideation," Amnesty International Report POL 40/7350/2023, https://www.amnesty.org/en/documents/pol40/7350/2023/en (November 7, 2023).

Amnesty International, 'I feel exposed': Caught in TikTok's surveillance web," Amnesty International Report POL 40/7349/2023, https://www.amnesty.org/en/documents/pol40/7349/2023/en (November 7, 2023).

Jeff Amy, "Georgia, NH latest states to ban TikTok from state computers," AP News, https://apnews.com/article/technology-georgia-8e62e34976ef070a9e24305248981684 (December 15, 2022).

Jamil Anderlini and Clothilde Goujard, "Brussels moves to ban Eurocrats from using TikTok," *Politico*, https://www.politico.eu/article/european-commission-to-staff-dont-use-tiktok (February 23, 2023).

* Lawrence Andrea, "Gov. Tony Evers issues order banning TikTok on most state-issued devices," *Milwaukee Journal Sentinel*, https://www.jsonline.com/story/news/politics/2023/01/12/tony-evers-issues-order-banning-tiktok-on-some-state-issued-devices/69803482007 (January 12, 2023).

Associated Press, "Louisiana's secretary of state bans TikTok on devices issued by Department of State," FOX News, https://www.foxnews.com/us/louisianas-secretary-state-bans-tiktok-devices-issued-department-state (December 20, 2022).

Associated Press, "Maine is the latest state to ban TikTok for state workers," AP News, https://apnews.com/article/politics-maine-state-government-china-business-734ce1f1abde9c3b2a9c8172c6763d01 (January 19, 2023).

Associated Press, "TikTok blocked from Indiana state devices," WTHR, https://www.wthr.com/article/news/local/indiana-blocks-chinese-owned-app-tiktok-from-state-devices-social-media/531-7bb0ccc2-29b2-47bb-a1be-71aa836b03b3 (December 30, 2022).

Association for Computing Machinery, "ACM code of ethics and professional conduct," https://www.acm.org/code-of-ethics (June 22, 2018).

Association for Computing Machinery, U.S. Public Policy Council, "USACM statement on the importance of preserving personal privacy," https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf (March 1, 2018).

Australian Information Commissioner, "Statement on TikTok preliminary inquiries," https://www.oaic.gov.au/news/media-centre/statement-on-tiktok-preliminary-inquiries (May 29, 2024).

Gavin Bade, "Lawmakers shift gears on TikTok ban," *Politico*, https://www.politico.com/news/2023/10/09/what-happened-to-the-tiktok-ban-00120434 (October 9, 2023).

Frank Bajak and Dake Kang, "Leaked hacking files show Chinese spying on citizens and foreigners alike," *PBS News*, https://www.pbs.org/newshour/world/leaked-hacking-files-show-chinese-spying-on-citizens-and-foreigners-alike (February 21, 2024).

Emily Baker-White, "Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China," *BuzzFeed News*, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access (June 17, 2022).

* Emily Baker-White, "TikTok parent ByteDance planned to use TikTok to monitor the physical location of specific American citizens," *Forbes*. https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=1dba4cfb6c2d (October 20, 2022).

* Emily Baker-White, "A zero day TikTok hack is taking over celebrity and brand accounts," https://www.forbes.com/sites/emilybaker-white/2024/06/04/a-zero-day-tiktok-hack-is-taking-over-celebrity-and-brand-accounts (June 4, 2024).

James Ball (April 20, 2012), "Hacktivists in the frontline battle for the internet," *The Guardian*, https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet (April 20, 2012).

Elaine Barker et al., "A framework for designing cryptographic key management systems," NIST Special Publication 800-130, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf (August 2013).

* John Perry Barlow, "Jackboots on the Infobahn," *Wired*, https://www.wired.com/1994/04/privacy-barlow (April 1, 1994).

* Julian E. Barnes and Edward Wong, "Chinese hackers targeted Commerce Secretary and other U.S. Officials," *New York Times*, https://www.nytimes.com/2023/07/12/us/politics/china-state-department-emails-microsoft-hack.html (July 12, 2023).

* Devlin Barrett, "Chinese national arrested for allegedly using malware linked to OPM hack," *Washington Post*, https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html (August 24, 2017).

Ryan Barwick, "Advertisers are asking questions about the data TikTok can collect," *Marketing Brew*, https://www.marketingbrew.com/stories/2022/11/22/advertisers-are-asking-questions-about-the-data-tiktok-can-collect (November 22, 2022).

Christopher Bing, "Clues in Marriott hack implicate China - sources," Reuters, https://www.reuters.com/article/world/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504R/ (December 6, 2018).

Paul Bischoff, "Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and Youtube," *Comparitech*, https://www.comparitech.com/blog/information-security/social-data-leak (May 30, 2021).

Richard Blumenthal and Marsha Blackburn, Letter to Avril Haines, Director of National Intelligence, https://www.blumenthal.senate.gov/imo/media/doc/3212024odnitiktokdeclassification.pdf (March 21, 2024).

Richard Blumenthal and Marsha Blackburn, Letter to Shou Zi Chew, Chief Executive Officer, TikTok, https://www.blackburn.senate.gov/services/files/76E769A8-3EDA-4BA0-989E-42D5F99E547D (June 6, 2023).

Laura Brandimarte, Alessandro Acquisti and George Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science* 4, no. 3, https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf (May 2013).

Ashley Burke, "Canada targeted by same Chinese hackers the U.S., U.K. accuse of cyberespionage that hit millions," CBC, https://www.cbc.ca/news/world/cyberespionage-china-hack-canada-targetted-1.7155482 (March 26, 2024).

* Cate Cadell, "China harvests masses of data on Western targets, documents show," *Washington Post*, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-

western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html (December 31, 2021).

California Constitution, "Article 1 Declaration of Rights," California Legislative Information, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

California Consumer Privacy Act, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (effective January 1, 2020).

Benjamin Carlson, "Quote of the day: Google CEO compares data across millennia," *The Atlantic*, https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989 (July 3, 2010).

Check Point Research, "Pandas with a soul: Chinese espionage attacks against Southeast Asian government entities," https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities (March 7, 2023).

China Law Translate, "PRC National Intelligence Law," https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017 (June 27, 2017).

Kevin Collier and Scott Wong, "White House backs bipartisan bill that could be used to ban TikTok," NBC News, https://www.nbcnews.com/tech/tech-news/restrict-act-bill-tiktok-rcna73682 (March 7, 2023) (RESTRICT Act).

Colorado Privacy Act, https://leg.colorado.gov/bills/sb21-190 (effective July 1, 2023).

Connecticut Personal Data Privacy and Online Monitoring Act, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022 (effective July 1, 2023).

Eva Corlett, "New Zealand parliament targeted in China-backed hack in 2021, spy agency says," *The Guardian*, https://www.theguardian.com/world/2024/mar/26/new-zealand-parliament-china-hack-2021-spy-agency-gcsb (March 25, 2024).

Council of Europe, "European Convention on Human Rights," https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953) ("Everyone has the right to respect for his private and family life, his home and his correspondence").

Chris Crum, "Google eyes mouse movement as possible search relevancy signal," *WebProNews*, https://www.webpronews.com/google-eyes-mouse-movement-as-possible-search-relevancy-signal (July 13, 2010).

Cybersecurity and Infrastructure Security Agency, "People's Republic of China-linked cyber actors hide in router firmware," https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a (September 27, 2023).

Alexandre Côté Cyr, "MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT," *WeLiveSecurity*, ESET, https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt (March 2, 2023).

* Sopan Deb, "Ticketmaster confirms data breach. Here's what to know," *New York Times*, https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html (May 31, 2024).

Mack DeGuerin, "TikTok owner admits employees accessed data of U.S. users and journalists," *Gizmodo*. https://gizmodo.com/tiktok-data-china-bytedance-1849924671 (December 22, 2022)

Ron Deibert, Post, *X*, https://x.com/RonDeibert/status/1631099697635926019 (March 1, 2023).

Delaware Personal Data Privacy Act, https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=140388&legislationTypeId=1&docTypeId=2&legislationName=HB154 (effective January 1, 2025).

Samantha Delouya, "Montana governor bans TikTok," CNN Business, https://www.cnn.com/2023/05/17/tech/montana-governor-tiktok/index.html (May 18, 2023).

* Karoun Demirjian, "Chinese hackers stole 60,000 State Dept. emails in breach reported in July," *New York Times*, https://www.nytimes.com/2023/09/27/us/politics/chinese-hackers-state-department.html (September 27, 2023).

* Zak Doffman, "Ashley Madison hack returns to 'haunt' its victims: 32 million users now watch and wait," *Forbes*, https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait (February 1, 2020).

* Alison Durkee, "TikTok ban heard today in court—Here's what to know," *Forbes*, https://www.forbes.com/sites/alisondurkee/2024/09/16/tiktok-ban-heard-today-in-court-heres-what-to-know (September 16, 2024).

Peter Eckersley, "How unique is your web browser?" *Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin*, https://coveryourtracks.eff.org/static/browser-uniqueness.pdf (July 2010).

Steven Englehardt, et al., "Cookies that give you away: The surveillance implications of web tracking," *WWW '15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).

Frank Esposito, "Cashless tolls: Welcome to the dark future," *Rockland/Westchester Journal News*, https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002 (April 11, 2018).

European Commission, "General Data Protection Regulation: Art. 5 GDPR: Principles relating to processing of personal data," https://gdpr-info.eu/art-5-gdpr (enacted April 5, 2016; effective May 25th, 2018).

European Union, "Charter of Fundamental Rights of The European Union," https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).

European Union, "General data protection regulation (GDPR)," https://gdpr-info.eu (April 27, 2016).

Tom Fakterman, "Chinese APT abuses VSCode to target government in Asia," Palo Alto Networks, https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage (September 6, 2024).

Stephen Farrell and Hannes Tschofenig, "Pervasive monitoring is an attack," *Best Current Practice* 188, Internet Engineering Task Force, https://datatracker.ietf.org/doc/html/rfc7258 (May 2014).

Müge Fazlioglu, "U.S. federal privacy legislation tracker," International Association of Privacy Professionals, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker (last updated August 2024).

Todd Feathers, Katie Palmer and Simon Fondrie-Teitler, "'Out of control': Dozens of telehealth startups sent sensitive health information to Big Tech companies," *The Markup*, https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (December 13, 2022).

Ed Felten, "Does hashing make data 'anonymous'?" Federal Trade Commission, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous (April 22, 2012).

FindLaw, "Is there a 'right to privacy' amendment?" https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html (last reviewed August 20, 2023).

Joel Finkelstein and Alex Goldenberg, "A Tik-Tok-ing timebomb: How TikTok's global platform anomalies align with the Chinese Communist Party's geostrategic objectives," Network Contagion Research Institute and Miller Center on Policing and Community Resilience, Rutgers University, https://networkcontagion.us/wp-content/uploads/A-Tik-Tok-ing-Timebomb_12.21.23.pdf (December 21, 2023).

Jim Finkle, "Massive data breach at Experian exposes personal data for 15 million T-Mobile customers," *Huffington Post*/Reuters, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).

Andrew Folks, "US State privacy legislation tracker," International Association of Privacy Professionals, https://iapp.org/resources/article/us-state-privacy-legislation-tracker (last updated July 22, 2024)

Jeremiah Fowler, "1.5 billion records leaked in Real Estate Wealth Network data breach," *Security InfoWatch*, https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach (December 26, 2023).

FOX 10 Phoenix, "Arizona Gov. Hobbs bans TikTok on state devices," FOX 10 Phoenix, https://www.fox10phoenix.com/news/arizona-gov-hobbs-bans-tiktok-on-state-devices (April 5, 2023).

Elaine Fox, "Response to the Data Protection Commission's Decision," TikTok, https://newsroom.tiktok.com/en-ie/response-to-the-data-protection-commission (September 27, 2023).

Jonathan Franklin, "New York City officially bans TikTok on all government devices," National Public Radio, https://www.npr.org/2023/08/17/1194422613/new-york-city-bans-tiktok-government-devices (August 17, 2023).

Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" *CSO Magazine*, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (February 12, 2020).

Hailey Fuchs, "Chinese diplomats are quietly meeting with Hill staffers about TikTok," *Politico*, https://www.politico.com/news/2024/04/17/china-lobbying-tiktok-congress-00152819 (April 17, 2024).

Brian Fung, "Biden just signed a potential TikTok ban into law. Here's what happens next," *CNN Business*, https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html (April 24, 2024).

Brian Fung, "FTC investigating TikTok over privacy and security," *CNN Business*, https://www.cnn.com/2024/03/26/tech/ftc-tiktok-probe-privacy-and-security/index.html (March 26, 2024).

Brian Fung, "Montana lawmakers vote to completely ban TikTok in the state," *CNN Business*, https://www.cnn.com/2023/04/14/tech/montana-house-tiktok-ban/index.html (April 14, 2020).

Brian Fung, "There is now some public evidence that China viewed TikTok data," *CNN Business*, https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html (June 8, 2023).

Jared Gans, "Youngkin joins GOP governors in banning TikTok on state devices, wireless networks," *The Hill*, https://thehill.com/homenews/state-watch/3778557-youngkin-joins-gop-governors-in-banning-tiktok-on-state-devices-wireless-networks (December 16, 2022).

Simson L. Garfinkel, "De-identification of personal information," NIST IR 8053, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf (October 2015).

Thomas Germain, "How TikTok tracks you across the web, even if you don't use the app," *Consumer Reports*, https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813 (September 29, 2022).

Thomas Germain, "We found 28,000 apps sending TikTok data. Banning the app won't help," *Gizmodo*, https://gizmodo.com/tiktok-ban-joe-biden-28000-apps-sdk-data-china-1850174019 (March 2, 2023).

Michael Goldberg, "Mississippi governor bans TikTok from government devices," AP News, https://apnews.com/article/politics-mississippi-state-government-tate-reeves-business-b3658341702baf2a49ab0afbb618ee98 (January 11, 2023).

Dan Goodin, "Backdoored firmware lets China state hackers control routers with "magic packets"," *Ars Technica*, https://arstechnica.com/security/2023/09/china-state-hackers-are-camping-out-in-cisco-routers-us-and-japan-warn (September 27, 2023).

Sasha Gressin, "The Marriott data breach," *Consumer Advice*, U.S. Federal Trade Commission, https://consumer.ftc.gov/consumer-alerts/2018/12/marriott-data-breach (December 4, 2018).

Stephen Groves, "South Dakota Gov. Noem bans TikTok from state-owned devices," AP News, https://apnews.com/article/south-dakota-bans-tiktok-from-state-devices-f7a95dd494dab9c410ff80c577c609dd (November 29, 2022).

The Guardian, "Chinese hackers infiltrated plane, train and water systems for five years, US says," *The Guardia*n, https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure (February 8, 2024).

* Alisha Haridasani Gupta and Natasha Singer, "Your app knows you got your period. Guess who it told?" *New York Times*, https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html (January 28, 2021).

Pieter Haeck, "Beyond TikTok, Dutch tell government staff to uninstall Chinese, Russian apps," *Politico*, https://www.politico.eu/article/the-netherlands-china-russia-cyber-security-xi-jinping-vladimir-putin-recommends-officials-to-uninstall-apps (March 21, 2023).

Liam Halawith, "Gov. Kim Reynolds bans TikTok on state-owned devices," *Daily Iowan*, https://dailyiowan.com/2022/12/14/governor-kim-reynolds-bans-tiktok-on-state-owned-devices (December 14, 2022).

Madison Hall, "China just proved why Congress wants to ban TikTok," *Business Insider*, https://www.businessinsider.com/china-just-proved-why-congress-wants-to-ban-tiktok-2024-4 (April 17, 2024).

John Hanna, "Kansas' Democratic governor imposes TikTok ban," AP News, https://apnews.com/article/kansas-tik-tok-ban-explainer-83ef9bc3ff44d90e7b0f54bd8f5228cb (December 28, 2022).

* Amy Harmon, "As public records go online, some say they're too public," *New York Times*, https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html (August 24, 2001).

* Drew Harwell, "Montana ban on TikTok blocked, extending critics' losing streak," *Washington Post*, https://www.washingtonpost.com/technology/2023/11/30/tiktok-ban-montana-blocked (November 30, 2023).

* Drew Harwell, "TikTok and the U.S. government dig in for a legal war over potential ban," *Washington Post*, https://www.washingtonpost.com/technology/2024/04/25/tiktok-legal-battle-is-certain (April 25, 2024).

Amy Hawkins, "Huge cybersecurity leak lifts lid on world of China's hackers for hire," *The Guardian*, https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire (February 23, 2024).

Alex Hern and Aletha Adu, "TikTok fined £12.7m for illegally processing children's data." *The Guardian*. https://www.theguardian.com/technology/2023/apr/04/tiktok-fined-uk-data-protection-law-breaches (April 4, 2023).

Alex Hern, "Revealed: how TikTok censors videos that do not please Beijing," *The Guardian*, https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing (September 25, 2019).

Alex Hern, "TikTok's local moderation guidelines ban pro-LGBT content," *The Guardian*, https://www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content (September 26, 2019).

Aaron Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online," *Business Insider*, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (April 3, 2021).

* Raffaele Huang, "TikTok's efforts to distance itself from Chinese parent stumble over talent," *Wall Street Journal*, https://www.wsj.com/articles/tiktoks-efforts-to-cut-ties-with-chinese-parent-stumble-over-talent-11671186110 (December 16, 2022).

Kaia Hubbard, "TikTok is a "national security issue," Sens. Mark Warner and Marco Rubio say," *CBS News*, https://www.cbsnews.com/news/tiktok-national-security-issue-mark-warner-marco-rubio-senate-intelligence-committee (March 10, 2024).

E.E. Hutchinson, "Keeping your personal information personal: Trouble for the modern consumer," 43 Hofstra L.Rev. 1151, 1168, https://scholarlycommons.law.hofstra.edu/hlr/vol43/iss4/7 (January 1, 2015).

Sumeyya Ilanbey and David Swan, "Australian companies dump TikTok tracking tool amid privacy concerns," *Sydney Morning Herald*, https://www.smh.com.au/business/companies/australian-companies-dump-tiktok-tracking-tool-amid-privacy-concerns-20240110-p5ewc0.html (January 15, 2024).

Sumeyya Ilanbey and David Swan, "Australian companies dump TikTok tracking tool amid privacy concerns," *Sydney Morning Herald*,

https://www.smh.com.au/business/companies/australian-companies-dump-tiktok-tracking-tool-amid-privacy-concerns-20240110-p5ewc0.html (January 15, 2024).

Indiana Consumer Data Protection Act, https://iga.in.gov/pdf-documents/123/2023/senate/bills/SB0005/SB0005.05.ENRH.pdf (effective January 1, 2026).

David Ingram, "Biden signs TikTok ban for government devices, setting up a chaotic 2023 for the app," NBC News, https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724 (December 30, 2022).

International Association of Privacy Professionals, "What is privacy?" https://iapp.org/about/what-is-privacy (2024).

International Organization for Standardization, "Information technology: Vocabulary," ISO/IEC 2382:2015, https://www.iso.org/obp/ui/en/#!iso:std:63598:en (May 2015).

Iowa Consumer Data Protection Act, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262 (effective January 1, 2025).

Irish Data Protection Commission, "Irish Data Protection Commission announces €345 million fine of TikTok," https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok (September 15, 2023).

Chris Jackson and Catherine Morris, "Americans report high levels of concern about data privacy and security," *Ipsos,* https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security (March 16, 2021).

Scott Jasper, "Chinese and Russian legitimate tool attacks mandate AI-enabled cyber defenses," The Cyber Edge, https://www.afcea.org/signal-media/cyber-edge/chinese-and-russian-legitimate-tool-attacks-mandate-ai-enabled-cyber (May 1, 2024).

* Jacob Judah, "Why a Pacific island is blaming China for a hack?" *New York Times*, https://www.nytimes.com/2024/06/02/world/asia/palau-taiwan-china-hack.html (June 2, 2024).

Divya Karthikeyan, "TikTok banned from Kentucky government devices," WKMS, https://www.wkms.org/government-politics/2023-01-16/tiktok-banned-from-kentucky-government-devices (January 16, 2023).

Michael Kassner, "Anatomy of the Target data breach," *ZD Net*, https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned (February 2, 2015).

Kentucky Consumer Data Protection Act, https://apps.legislature.ky.gov/law/acts/24RS/documents/0072.pdf (effective January 1, 2026).

Rebecca Kern, "TikTok's biggest threat just passed the House," *Politico*, https://www.politico.com/news/2024/03/13/tiktok-ban-bill-house-passes-00146720 (March 13, 2024).

Daniel Konstantinovic, "ByteDance revenues rival Meta as both compete over social commerce," *eMarketer*, https://www.emarketer.com/content/bytedance-revenues-rival-meta-both-compete-over-social-commerce (November 15, 2023).

Brian Krebs, "Experian API exposed credit scores of most Americans," *Krebs on Security*, https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans (April 28, 2021).

Kelly Laco, "Sarah Huckabee Sanders bans TikTok on state devices in first move as Arkansas governor," FOX News, https://www.foxnews.com/politics/sarah-huckabee-sanders-bans-tiktok-state-devices-first-move-arkansas-governor (January 10, 2023).

Ravie Lakshmanan, "Chinese hackers exploit Visual Studio code in Southeast Asian cyberattacks," *The Hacker News*, https://thehackernews.com/2024/09/chinese-hackers-exploit-visual-studio.html (September 9, 2024)/

Ravie Lakshmanan, "Chinese hackers launch covert espionage attacks on 24 Cambodian organizations," *The Hacker News*, https://thehackernews.com/2023/11/chinese-hackers-launch-covert-espionage.html (November 13, 2023).

Ravie Lakshmanan, "Chinese hackers using SugarGh0st RAT to target South Korea and Uzbekistan," *The Hacker News*, https://thehackernews.com/2023/12/chinese-hackers-using-sugargh0st-rat-to.html (December 1, 2023).

Ravie Lakshmanan, "Chinese Redfly group compromised a nation's critical grid in 6-month ShadowPad campaign," *The Hacker News*, https://thehackernews.com/2023/09/chinese-redfly-group-compromised.html (September 12, 2023).

Ravie Lakshmanan, "Daggerfly cyberattack campaign hits African telecom services providers," *The Hacker News*, https://thehackernews.com/2023/04/daggerfly-cyberattack-campaign-hits.html (April 20, 2023).

Ravie Lakshmanan, "Guyana governmental entity hit by DinodasRAT in cyber espionage attack," *The Hacker News,* https://thehackernews.com/2023/10/guyana-governmental-entity-hit-by.html (October 5, 2023).

Ravie Lakshmanan, "Microsoft thwarts Chinese cyber attack targeting western European governments," *The Hacker News*, https://thehackernews.com/2023/07/microsoft-thwarts-chinese-cyber-attack.html (July 12, 2023).

Ravie Lakshmanan, "Mustang Panda hackers targets Philippines government amid South China Sea tensions," *The Hacker News*, https://thehackernews.com/2023/11/mustang-panda-hackers-targets.html (November 21, 2023).

Ravie Lakshmanan, "Pakistani entities targeted in sophisticated attack deploying ShadowPad malware," *The Hacker News*, https://thehackernews.com/2023/07/pakistani-entities-targeted-in.html (July 18, 2023).

Selena Larson, "Every single Yahoo account was hacked—3 billion in all," *CNN Business,* https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (October 4, 2017).

Nate Lavoy, "TikTok is a threat to national security, but not for the reason you think," Rand Corporation, https://www.rand.org/pubs/commentary/2024/08/tiktok-is-a-threat-to-national-security-but-not-for.html (August 14, 2024).

Joseph J. Lazzarotti and Mary T. Costigan, "CCPA FAQs on cookies," *National Law Review* 13, no. 52, https://www.natlawreview.com/article/ccpa-faqs-cookies (August 29, 2019).

Sara Lebow, "Guide: TikTok," Emarketer. https://www.emarketer.com/insights/guide-tiktok (July 18, 2024).

* Rachel Lerman and Cristiano Lima-Strong, "TikTok, Snap, YouTube defend how they protect kids online in congressional hearing," *Washington Post*, https://www.washingtonpost.com/technology/2021/10/26/tiktok-snapchat-youtube-congress-hearing (October 26, 2021).

Adam Lerner, et al., "Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016," 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner (2016).

* Alexandra Levine, "TikTok creators' sensitive financial information stored in China," *Forbes*, https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china (May 30, 2023).

* Alexandra Levine, "TikTok hit with $370M fine in Europe over children's privacy missteps," *Forbes*, https://www.forbes.com/sites/alexandralevine/2023/09/14/tiktok-fine-europe-children-data-privacy-security (September 15, 2023).

* Alexandra Levine, "TikTok mishandled the data of hundreds of top American advertisers," *Forbes*, https://www.forbes.com/sites/alexandralevine/2024/04/17/tiktok-mishandled-advertisers-data-bytedance-china (April 17, 2024).

Pellaeon Lin, "TikTok vs Douyin: A security and privacy analysis," Research Report 137, *Citizen Lab*, https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis (March 22, 2021).

Brad Little, "Gov. Little bans TikTok on state-issued devices," *East Idaho News*, https://www.eastidahonews.com/2022/12/gov-little-bans-tiktok-on-state-issued-devices (December 14, 2022).

LOKKER, “Website privacy and compliance challenges: Qualifying website privacy risks,” https://lokker.com/wp-content/uploads/2024/04/LOKKER_Online-Data-Privacy-Report_032024-2.pdf (March 2024).

Qiao Long, “China setting up 'grid' system to monitor ordinary people,” *Radio Free Asia*, https://www.rfa.org/english/news/china/china-setting-up-grid-system-to-monitor-ordinary-people-04102018121018.html (April 10, 2018).

Ryan Love, “Oklahoma Gov. Stitt bans TikTok on government devices,” KJRH, https://www.kjrh.com/news/local-news/oklahoma-gov-stitt-bans-tiktok-on-government-devices (December 28, 2022).

Andrew Macaskill and James Pearson, “Britain says China hacked electoral watchdog, targeted lawmaker emails,” Reuters, https://www.reuters.com/world/uk/uk-deputy-pm-set-address-lawmakers-chinese-cyber-security-threat-2024-03-24 (March 25, 2024).

* Sapna Maheshwari and Ryan Mac, "Driver’s licenses, addresses, photos: Inside how TikTok shares user data," *New York Times*, https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html (May 24, 2023).

* Sapna Maheshwari, “Love, hate or fear it, TikTok has changed America,” *New York Times*, https://www.nytimes.com/interactive/2024/04/18/business/media/tiktok-ban-american-culture.html (April 19, 2024).

* Sapna Maheshwari, “Senators say TikTok may have misled Congress on handling of U.S. user data,” *New York Times*, https://www.nytimes.com/2023/06/07/technology/tiktok-congress-user-data.html (June 7, 2023).

* Sapna Maheshwari, “Topics suppressed in China are underrepresented on TikTok, study says,” *New York Times*, https://www.nytimes.com/2023/12/21/business/tiktok-china.html (December 21, 2023).

Angelica Mari, “Experian challenged over massive data leak in Brazil,” *ZD Net*, https://www.zdnet.com/article/experian-challenged-over-massive-data-leak-in-brazil (February 20, 2021).

Maryland Online Data Privacy Act, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0541 (effective October 1, 2025).

Massachusetts Data Privacy Protection Act (Bill S.2770) in, https://malegislature.gov/Bills/193/S2770.pdf (introduced February 16, 2023; revised bill submitted May 9, 2024).

Colleen McClain, “About half of TikTok users under 30 say they use it to keep up with politics, news,” Pew Research Center, https://www.pewresearch.org/short-reads/2024/08/20/about-half-of-tiktok-users-under-30-say-they-use-it-to-keep-up-with-politics-news (August 20, 2024).

Megan McCluskey, "TikTok has started collecting your 'faceprints' and 'voiceprints.' Here's what it could do with them," *TIME*, https://time.com/6071773/tiktok-faceprints-voiceprints-privacy (June 14, 2021).

* Joseph Menn, "Chinese spies who read State Dept. email also hacked GOP congressman," *Washington Post*, https://www.washingtonpost.com/technology/2023/08/14/microsoft-china-hack-congress (August 15, 2023).

* Joseph Menn, "U.S. says Chinese hackers breached gear in Guam, key to Pacific defense," *Washington Post*, https://www.washingtonpost.com/technology/2023/05/24/china-hack-guam-taiwan.

Meta Platforms, Inc., "Form 10-K," United States Securities and Exchange Commission, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf (February 3, 2023).

Michigan Personal Data Privacy Act (SB 1182), https://legislature.mi.gov/Bills/Bill?ObjectName=2022-SB-1182 (introduced September 27, 2022).

Microsoft Security Response Center, "Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email," *MSRC Blog*, https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email (July 11, 2023).

Microsoft Threat Intelligence, "Flax Typhoon using legitimate software to quietly access Taiwanese organizations," *Microsoft Security Blog*, https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations (August 24, 2023).

Microsoft Threat Intelligence, "Same targets, new playbooks: East Asia threat actors employ unique method," Microsoft, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf (April 2024).

Aleksandar Milenkoski et al., "Operation Tainted Love: Chinese APTs target telcos in new attacks," Sentinel Labs, https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks (March 23, 2023)

Minnesota Consumer Data Privacy Act, https://www.revisor.mn.gov/bills/text.php?number=HF4757&type=bill&version=4&session=ls93&session_year=2024&session_number=0&format=pdf (effective July 31, 2025).

Montana 68th Legislature 2023, "An act banning TikTok in Montana," SB0419, https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf (effective January 1, 2024).

Montana Consumer Data Privacy Act, https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf (effective October 1, 2024).

* Paul Mozur and Aaron Krolik, "A surveillance net blankets China's cities, giving police vast powers," *New York Times*, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html (December 17, 2019).

Phil Muncaster, "Experian data breach hits 24 million customers," *InfoSecurity Magazine*, https://infosecurity-magazine.com/news/experian-data-breach-24-million (August 20, 2020).

Facundo Muñoz, "The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia," *WeLiveSecurity*, ESET, https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia (March 14, 2023).

Julia Musto, "North Dakota governor bans TikTok app in executive branch agencies," *FOX Business*, https://www.foxbusiness.com/technology/north-dakota-governor-bans-tiktok-app-executive-agencies (December 14, 2022).

* Ellen Nakashima, "China hacked Japan's sensitive defense networks, officials say," *Washington Post*, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon (August 8, 2023).

* Ellen Nakashima and Joseph Menn, "China's cyber army is invading critical U.S. services," *Washington Post*, https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict (December 11, 2023).

* Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say (July 9, 2015).

NBCDFW, "Gov. Abbott bans TikTok on state-issued devices over cybersecurity concerns," NBC Dallas-Fort Worth, https://www.nbcdfw.com/news/local/texas-news/gov-abbott-bans-tiktok-on-state-issued-laptops-phones-and-other-devices/3143349 (December 7, 2022).

Nebraska Data Privacy Act, https://nebraskalegislature.gov/bills/view_bill.php?DocumentID=54904 (effective January 1, 2025).

Stephen Neukam, "NJ governor bans TikTok on state devices," *The Hill*, https://thehill.com/homenews/state-watch/3805699-nj-governor-bans-tiktok-on-state-devices/ (January 9, 2023).

New Hampshire SB 255, https://gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1 (effective January 1, 2025).

New Jersey SB 332, https://www.njleg.state.nj.us/bill-search/2022/S332 (effective January 15, 2025).

Lily Hay Newman, "US TikTok user data has been repeatedly accessed from China, leaked audio shows," *WIRED*, https://www.wired.com/story/leaky-forms-keyloggers-meta-tiktok-pixel-study (May 11, 2022).

Meredith Newman, "Delaware bans the use of TikTok on state devices due to cybersecurity concerns," *Delaware News Journal*, https://www.delawareonline.com/story/news/politics/2023/02/09/delaware-bans-tiktok-on-state-devices/69888579007 (February 9, 2023).

Office of the Attorney General, "Attorney General Bonta announces nationwide investigation into TikTok," California Department of Justice, Office of the Attorney General, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-nationwide-investigation-tiktok (March 2, 2022).

Office of the Attorney General, "California Consumer Privacy Act," https://oag.ca.gov/privacy/ccpa (accessed February 20, 2023).

Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (February 7, 2022).

Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (February 6, 2023).

Office of the Director of National Intelligence, "Annual threat assessment of the U.S. intelligence community," https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (February 5, 2024).

Office of the Privacy Commissioner of Canada, "Commissioners launch joint investigation into TikTok," https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230223 (February 23, 2023).

Ohio Personal Privacy Act (HB 376), https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA134-HB-376 (introduced July 12, 2021).

Arthur E. Oldehoeft, "Foundations of a security policy for use of the national research and educational network," NIST IR 4734, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4734.pdf (February 1992).

Lukasz Olejnik, Claude Castelluccia and Artur Janc, "Why Johnny can't browse in peace: On the uniqueness of web browsing history patterns," *Annals of Telecommunications* 1-2, https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf (June 2013).

Open AI, "Disrupting malicious uses of AI by state-affiliated threat actors," https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors (February 14, 2024).

Oregon Consumer Privacy Act, https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled (effective July 1, 2024).

Organization for Economic Cooperation and Development, "The OECD privacy framework," http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

Olafimihan Oshin, "Hogan orders TikTok ban for Maryland government employees," *The Hill*, https://thehill.com/policy/technology/3764025-hogan-orders-tiktok-ban-for-maryland-government-employees (December 6, 2022).

Olafimihan Oshin, "Utah governor orders TikTok ban for state government employees," *The Hill*, https://thehill.com/homenews/state-watch/3772150-utah-governor-orders-tiktok-ban-for-state-government-employees (December 12, 2022).

Oxford English Dictionary Online, "Private" (retrieved September 6, 2024).

Frank Pasquale, "The troubling trend toward trade secret-protected ranking systems," Chicago Intellectual Property Colloquium, Chicago, Illinois, https://blogs.kentlaw.iit.edu/wp-content/uploads/sites/36/files/2016/12/pasquale.pdf (April 21, 2009).

James Pearson and Anthony Deutsch, "Chinese spies hacked Dutch defence network last year—intelligence agencies," Reuters, https://www.reuters.com/technology/cybersecurity/china-cyber-spies-hacked-computers-dutch-defence-ministry-report-2024-02-06 (February 6, 2024).

James Pearson, Raphael Satter and Christopher Bing, "US, UK accuse China of cyberespionage that hit millions of people," Reuters, https://www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25 (March 25, 2024).

Minxin Pei, "China's 1% is watching the other 99%," *Bloomberg*, https://www.bloomberg.com/opinion/articles/2024-02-04/china-s-surveillance-state-depends-on-people-not-cameras (February 4, 2024).

Minxin Pei, "Grid management: China's latest institutional tool of social control," *China Leadership Monitor*, https://www.prcleader.org/post/grid-management-china-s-latest-institutional-tool-of-social-control (March 1, 2021).

Minxin Pei, *The Sentinel State*, Harvard University Press, https://www.hup.harvard.edu/books/9780674257832 (February 13, 2024).

Helen A.S. Popkin, "Life is too short to read privacy policies - here's statistical proof!" NBC News, https://www.nbcnews.com/tech/tech-news/life-too-short-read-privacy-policies-heres-statistical-proof-flna297399 (March 2, 2012).

PrivacyTools.io, "Exodus for Android: Finds trackers embedded in all your apps," https://www.privacytools.io/guides/exodus-for-android-finds-trackers (accessed September 9, 2024).

Reuters, "Germany accuses China of conducting 2021 cyberattack on cartography agency," Reuters, https://www.reuters.com/world/germany-summons-chinese-ambassador-over-2021-cyberattack-cartography-agency-2024-07-31 (July 31, 2024).

Reuters, "Head of Belgian Foreign Affairs Committee says she was hacked by China," Reuters, https://www.reuters.com/world/europe/head-belgian-foreign-affairs-committee-says-she-was-hacked-by-china-2024-04-25 (April 25, 2024).

Reuters, "TikTok admits using its app to spy on reporters in effort to track leaks," *The Guardian*, https://www.theguardian.com/technology/2022/dec/22/tiktok-bytedance-workers-fired-data-access-journalists (December 23, 2022).

Rhode Island Data Transparency and Privacy Protection Act, https://fpf.informz.net/z/cjUucD9taT00MjA3NjkzJnA9MSZ1PTQzNzQ3OTU0MCZsaT00Njk5MDQ2Mw/index.html (effective January 1, 2026).

Charles Riley, "Insurance giant Anthem hit by massive data breach," *CNN Business*, https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security (February 6, 2015).

Aajene Robinson, "Alabama Gov. Kay Ivey bans TikTok on state devices," WBRC, https://www.wbrc.com/2022/12/14/alabama-gov-kay-ivey-bans-tiktok-state-devices (December 14, 2022).

Salvador Rodriguez, "TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance," CNBC, https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html (June 25, 2021).

Aaron Ross, James Pearson and Christopher Bing, "Chinese hackers attacked Kenyan government as debt strains grew," Reuters, https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24 (May 24, 2023).

Antoaneta Roussi and Pieter Haeck, "Ex-Belgian PM Guy Verhofstadt was a victim of Chinese hacking ," *Politico*, https://www.politico.eu/article/ex-belgian-pm-guy-verhofstadt-was-a-victim-of-chinese-hacking (April 20, 2024).

Lotus Ruan, "When the winner takes it all: Big data in China and the battle for privacy," Australian Strategic Policy Institute, https://www.aspi.org.au/report/big-data-china-and-battle-privacy (June 22, 2018).

Dominic Rush, "OPM hack: China blamed for massive breach of US government data," *The Guardian*, https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances (June 5, 2015).

Iris Samuels, "Alaska bans the use of TikTok on state-owned devices," *Anchorage Daily News*, https://www.adn.com/politics/2023/01/06/alaska-bans-the-use-of-tiktok-on-state-owned-devices/ (January 6, 2023).

* David E. Sanger, "Hackers took fingerprints of 5.6 million U.S. workers, government says," *New York Times*, https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html (September 23, 2015).

Megan Sauer, "Some TikTok users are receiving $167 checks over data privacy violations—and Google and Snapchat could be next," CNBC, https://www.cnbc.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html (October 28, 2022).

Bruce Schneier, *Data and Goliath,* Norton, https://archive.org/details/datagoliathhidde0000schn (2015).

Mathew J. Schwartz, "Google Aurora hack was Chinese counterespionage operation," *Dark Reading*, https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation (May 21, 2013).

Asuman Senol et al., "Leaky forms: A Study of email and password exfiltration before form submission," USENIX Security 2022, Boston, Massachusetts, August 10-12, 2022, https://homes.esat.kuleuven.be/%7Easenol/leaky-forms/leaky-forms-usenix-sec22.pdf (paper published March 13, 2022); follow-up study described at https://homes.esat.kuleuven.be/~asenol/leaky-forms/#advanced_matching (March 25, 2022).

Lauren Sforza, "Ohio joins list of states banning TikTok on government electronic devices," *The Hill*, https://thehill.com/homenews/state-watch/3805512-ohio-joins-list-of-states-banning-tiktok-on-government-electronic-devices (January 9, 2023).

David Shepardson, "Virginia, other US states back Montana in TikTok ban - court filing," Reuters, https://www.reuters.com/legal/virginia-other-us-states-back-montana-tiktok-ban-court-filing-2023-09-18 (September 18, 2023).

Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, https://books.google.com/books/about/Three_Felonies_a_Day.html?id=2xkDvMQlh-YC&source=kp_book_description (2011).

Zach Simas, "Unpacking the MOVEit Breach: Statistics and Analysis," EmsiSoft, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis (July 18, 2023; updated June 28, 2024).

* Natasha Singer, "Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome," *New York Times*, https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html (June 16, 2012).

Josh Sisco, "TikTok's troubles just got worse: The FTC could sue them, too," *Politico*, https://www.politico.com/news/2024/03/26/biden-administration-tiktok-data-practices-00149139 (March 26, 2024).

Antoinette Siu, "TikTok can circumvent Apple and Google privacy protections and access full user data, 2 studies say (Exclusive)," *Yahoo! News*, https://www.yahoo.com/entertainment/tiktok-circumvent-apple-google-privacy-140000271.html (February 14, 2022).

Minda Smiley, "Social time spent by Generation Z," *eMarketer*, https://www.emarketer.com/content/social-time-spent-by-generation-2024 (March 29, 2024).

Murray Scot Tanner, "Beijing's new National Intelligence Law: From defense to offense," *Lawfare*, https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense (July 20, 2017).

* Didi Kirsten Tatlow, "Beijing retirees looking to keep active volunteer to walk the beat," *New York Times*, https://www.nytimes.com/2015/10/29/world/asia/beijing-china-volunteer-retiree-patrol.html (October 29, 2015).

* Byron Tau and Duston Volz, "U.S. state-government websites use TikTok trackers, review finds," *Wall Street Journal*, https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0 (March 21, 2023).

Tennessee Information Protection Act, https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073 (effective July 1, 2025).

Texas Data Privacy and Security Act, https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB4 (effective July 1, 2024).

Fred Thys, "Vermont state government bans TikTok on its devices," *VT Digger*, https://vtdigger.org/2023/02/20/vermont-state-government-bans-tiktok-on-its-devices (February 20, 2023).

TikTok, "Delivering on our US data governance," https://usds.tiktok.com/delivering-on-our-us-data-governance (January 24, 2023).

TikTok, "Privacy policy," https://www.tiktok.com/legal/privacy-policy-row (last updated August 19, 2024).

TikTok, "TikTok Business Products (Data) Terms," https://ads.tiktok.com/i18n/official/policy/business-products-terms (effective July 29, 2024).

TikTok, Letter to Senators Richard Blumenthal and Marsha Blackburn, https://www.blackburn.senate.gov/services/files/A4595D03-689A-43FF-ADBA-32C557DE3685 (June 16, 2023).

* Craig Timberg, "Brokers use 'billions' of data points to profile Americans," *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

U.K. Home Office, "UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity," https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity (March 25, 2024).

U.K. Information Commissioner's Office, "ICO fines TikTok £12.7 million for misusing children's data," https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data (April 4, 2023).

U.K. National Cyber Security Centre, "UK calls out China state-affiliated actors for malicious cyber targeting of UK democratic institutions and parliamentarians (March 25, 2024).

U.S. Congress, H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, https://www.congress.gov/bill/118th-congress/house-bill/7521 (March 13, 2024).

U.S. Congress, H.R.815 -- Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes https://www.congress.gov/bill/118th-congress/house-bill/815 (signed into law April 24, 2024).

U.S. Cybersecurity and Infrastructure Security Agency, "People's Republic of China state-sponsored cyber actor Living off the Land to evade detection," https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a (May 24, 2023).

U.S. Cybersecurity and Infrastructure Security Agency, "People's Republic of China (PRC) Ministry of State Security APT40 tradecraft in action," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a (July 8, 2024).

U.S. Cybersecurity and Infrastructure Security Agency, "PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure," https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a (February 7, 2024).

U.S. Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, https://www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf (November 2021).

U.S. Department of Justice, "40 officers of China's National Police charged in transnational repression schemes targeting U.S. residents," https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us (April 17, 2023).

U.S. Department of Justice, "Four Chinese Nationals working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including infectious disease research," https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion (July 19, 2021).

U.S. Department of Justice, "Justice Department sues TikTok and parent company ByteDance for widespread violations of children's privacy laws," https://www.justice.gov/opa/pr/justice-

department-sues-tiktok-and-parent-company-bytedance-widespread-violations-childrens (August 2, 2024).

U.S. Department of Justice, "Member of sophisticated China-based hacking group indicted for series of computer intrusions, including 2015 data breach of health insurer Anthem Inc. affecting over 78 million people," https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including (May 9, 2019).

U.S. Department of Justice, "Seven hackers associated with Chinese government charged with computer intrusions targeting perceived critics of China and U.S. businesses and politicians," https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived (March 25, 2024).

U.S. Department of Justice, "Seven international cyber defendants, including "Apt41" actors, charged in connection with computer intrusion campaigns against more than 100 victims globally," https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer (September 16, 2020).

U.S. Department of Justice, "Two Chinese hackers working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research," https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (July 21, 2020).

U.S. Department of Justice, "U.S. government disrupts botnet People's Republic of China used to conceal hacking of critical infrastructure," https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical (January 31, 2024).

U.S. Department of the Treasury, "Treasury sanctions China-linked hackers for targeting U.S. critical infrastructure," https://home.treasury.gov/news/press-releases/jy2205 (March 25, 2024).

U.S. District Court for the District of Columbia, Memorandum opinion, *TikTok v. Trump*, Case 1:20-cv-02658 (CJN), https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv2658-30 (September 27, 2020).

U.S. District Court for the Northern District of California, First amended complaint, *Misty Hong, et al., v. Bytedance, Inc., TikTok, Inc., et al*, Case 5:19-cv-07792-LHK, https://s3.documentcloud.org/documents/7012757/TikTok-MDL.pdf (May 11, 2020).

U.S. District Court for the Northern District of Illinois, Eastern Division, Consolidated amended class action complaint, *In re TikTok, Inc., Consumer Privacy Litigation*, Case 1:20-cv-04699, MDL No. 2948, https://www.documentcloud.org/documents/20492025-amended-complaint-tiktok-consumer-privacy-litigation (December 18, 2020).

U.S. District Court for the Northern District of Illinois, Eastern Division, Plaintiffs' motion for preliminary approval of class action settlement, *In re TikTok, Inc., Consumer Privacy Litigation*, Case 1:20-cv-04699, MDL No. 2948, https://s3.documentcloud.org/documents/20491862/plaintiffs-motion-for-preliminary-approval-of-class-action-settlement.pdf (February 25, 2021).

U.S. District Court, Eastern District of New York, Indictment, *U.S. v. Ni Gaobin et al.*, Case 24-CR-43, https://www.justice.gov/opa/media/1345141/dl?inline (January 30, 2024).

U.S. Executive Office of the President, "Big data: Seizing opportunities, preserving values," https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).

U.S. Federal Bureau of Investigation, "Chinese military hackers charged in Equifax breach," https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020 (February 10, 2020).

U.S. Federal Trade Commission, "No, hashing still doesn't make your data anonymous," https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous (July 24, 2024).

U.S. Federal Trade Commission, "Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law," https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy (February 27, 2019).

U.S. House of Representatives, Committee on Energy and Commerce, "TikTok: How Congress can safeguard American Data Privacy and protect children from online harms," Transcript of hearing held March 23, 2023, U.S. Government Publishing Office, https://www.congress.gov/118/chrg/CHRG-118hhrg53839/CHRG-118hhrg53839.pdf (March 23, 2023).

U.S. House of Representatives, Committee on Energy and Commerce, "TikTok: How Congress can safeguard American data privacy and protect children from online harms," Transcript of hearing held March 23, 2023, U.S. Government Publishing Office, https://www.congress.gov/118/chrg/CHRG-118hhrg53839/CHRG-118hhrg53839.pdf (March 23, 2023).

U.S. Senate, Committee on Commerce, Science and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security, "Subcommittee: Protecting Kids Online: Snapchat, TikTok, and YouTube," Transcript of hearing held October 26, 2021, https://www.govinfo.gov/content/pkg/CHRG-117shrg54901/pdf/CHRG-117shrg54901.pdf (October 26, 2021).

U.S. Supreme Court, "Decision," *United States v. Jones*, Case No. 10-1259, http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1 (January 23, 2012).

U.S. Office of the President, "Executive order on addressing the threat posed by TikTok," https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok (August 6, 2020).

Unit 42, "Chinese APT targeting Cambodian government," Palo Alto Networks, https://unit42.paloaltonetworks.com/chinese-apt-linked-to-cambodia-government-attacks (November 7, 2023).

United Nations, "Universal Declaration of Human Rights," https://www.un.org/en/about-us/universal-declaration-of-human-rights (December 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence").

United Nations Office of the High Commissioner for Human Rights, "The right to privacy in the digital age," https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx (2021).

* Bruce Upbin, "The web is much bigger (and smaller) than you think," *Forbes*, https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think (April 24, 2012).

Utah Consumer Privacy Act, https://le.utah.gov/~2022/bills/static/SB0227.html (effective December 31, 2023).

Brandon Vigliarolo, "China caught—again—with its malware in another nation's power grid," *The Register*, https://www.theregister.com/2023/09/12/china_malware_grid (September 12, 2023).

Brandon Vigliarolo, "Marriott Hotels admits to third data breach in 4 years," *The Register*, https://www.theregister.com/2022/07/06/marriott_hotels_suffer_yet_another (July 6, 2022).

Antonio Villas-Boas, "Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it's really you," *Business Insider*, https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7 (July 19, 2019).

Virginia Consumer Data Protection Act, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (effective January 1, 2023).

* Christian M. Wade, "Cashless tolls on Mass. Pike raise revenue, privacy concerns," *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).

Maya Wang, "China's algorithms of repression," Human Rights Watch, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass (May 1, 2019).

* Vivian Wang, "Xi Jinping's recipe for total control: An army of eyes and ears," *New York Times*, https://www.nytimes.com/2024/05/25/world/asia/china-surveillance-xi.html (May 25, 2024).

Clint Watts, "China, North Korea pursue new targets while honing cyber capabilities," *Microsoft on the Issues*, https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea (September 7, 2023)

Peter Watts, "The scorched earth society," Symposium of the International Association of Privacy Professionals, Toronto, Ontario, https://rifters.com/real/shorts/TheScorchedEarthSociety-transcript.pdf (May 9, 2014).

WBTV, "N.C. Gov. Cooper signs executive order initiating ban of TikTok, WeChat from state devices," WBTV, https://www.wbtv.com/2023/01/12/nc-gov-roy-cooper-signs-executive-order-initiating-ban-tiktok-wechat-state-devices (January 12, 2023).

* Sui-Lee Wee, "China uses DNA to track its people, with the help of American expertise," *New York Times*, https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html (February 21, 2019).

Zack Whittaker, "AT&T won't say how its customers' data spilled online," *TechCrunch*, https://techcrunch.com/2024/03/22/att-customers-data-leak-online (March 22, 2024).

Zack Whittaker, "Telehealth startup Cerebral shared millions of patients' data with advertisers," *TechCrunch*, https://techcrunch.com/2023/03/10/cerebral-shared-millions-patient-data-advertisers (March 10, 2023).

* Davey Winder, "235 million Instagram, TikTok and YouTube user profiles exposed in massive data leak," *Forbes*, https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=3a1f04331111 (August 19, 2020).

Leo Wolfson, "Wyoming Gov. Mark Gordon bans TikTok on all state owned devices," *Cowboy State Daily*, https://cowboystatedaily.com/2022/12/15/wyoming-gov-mark-gordon-bans-tiktok-on-all-state-owned-devices (December 15, 2022).

Scott Wong, Kate Santaliz and Liz Brown-Kaiser, "Momentum builds in Congress to crack down on TikTok," NBC News, https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998 (February 18, 2023).

Matthew Woodward, "TikTok user statistics: Everything you need to know," *Search Logistics*, https://www.searchlogistics.com/learn/statistics/tiktok-user-statistics (May 31, 2024).

WYFF, "TikTok off-limits for South Carolina employees on state devices, governor says," WYFF, https://www.wyff4.com/article/tiktok-south-carolina-employees-state-devices/42157146 (December 5, 2022).

Yuan Yang, "Belgium's cyber security agency links China to spear phishing attack on MP," *Financial Times*, https://www.ft.com/content/5c32261c-b1a6-488e-9002-0ca9e0c8ff1b (March 1, 2023).

* Cat Zakrzewski, Pranshu Verma and Claire Parker, "Texts, web searches about abortion have been used to prosecute women," *Washington Post*, https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution (July 3, 2022).

David Zetoony, Christian Auty and Karin Ross, "Answers to the most frequently asked questions concerning cookies and adtech," Bryan Cave Leighton Paisner, https://www.bclplaw.com/print/v2/content/1023613/ccpa-2020-answers-to-the-most-frequently-asked-questions-concerning-cookies-and-adtech.pdf (February 2020).

* Kim Zetter, "Google hackers targeted source code of more than 30 companies," *Wired*, https://www.wired.com/2010/01/google-hack-attack (January 13, 2010).

* Raymond Zhong, "China snares tourists' phones in surveillance dragnet by adding secret app," *New York Times*, https://www.nytimes.com/2019/07/02/technology/china-xinjiang-app.html (July 2, 2019).

* Raymond Zhong, "TikTok blocks teen who posted about China's detention camps," *New York Times*, https://www.nytimes.com/2019/11/26/technology/tiktok-muslims-censorship.html (November 26, 2019).

Shoshana Zuboff, *The Age of Surveillance Capitalism,* Public Affairs, https://openlibrary.org/books/OL26677236M/The_Age_of_Surveillance_Capitalism (2019), pp. 14, 17, 186.

Deposition Transcripts

Lizzie Li Transcript, dated June 5, 2024

Daniel Kirchgessner Transcript, dated April 17, 2024

Case Exhibits

TIKTOK_BG_000009045

TIKTOK_BG_000217358

TIKTOK_BG_000736841

TIKTOK_BG_000746271

TIKTOK-BG-000002930–940

TIKTOK-BG-000168680

TIKTOK-BG-000439076

Expert Reports

Declaration of Russell W. Mangum III, Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated June 21, 2024

Declaration of Zubair Shafiq Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated July 9, 2024

Expert Reply Report of Zubair Shafiq Ph. D. in Support of Plaintiffs' Motion for Class Certification, dated July 26, 2024

Responses to Interrogatories

Defendants' Amended Responses and Objections to Plaintiffs' Interrogatory No. 8

Defendants' Responses and Objections to Plaintiffs' Interrogatory No. 13

Defendants' Responses and Objections to Plaintiffs' Interrogatory No. 24

Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the *Economist*. He is the *New York Times* best-selling author of 16 books—including his latest, *A Hacker's Mind*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Professional Experience

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow and Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back, WW Norton & Co., 2023.

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Co., 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Co,, 2015.

13 additional books before August 2014.

Academic Publications

F. Heiding, B. Schneier, and A. Vishwanath, "AI Will Increase the Quantity—and Quality—of Phishing Scams," *Harvard Business Review*, May 30, 2024.

F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, P. S. Park, "Devising and Detecting Phishing Emails Using Large Language Models," *IEEE Access*, March 11, 2024.

B. Raghavan and B. Schneier, "A Bold New Plan for Preserving Online Privacy and Security: Decoupling Our Identities from Our Data and Actions Could Safeguard Our Secrets," *IEEE Spectrum*, December 2023.

N. E. Sanders, A. Ulinich, and B. Schneier, "Demonstrations of the Potential of AI-based Political Issue Polling," arXiv:2307.04781 [cs.CY], July 10, 2023.

J. Penney and B. Schneier, "Platforms, Encryption, and the CFAA: The Case of *WhatsApp v. NSO Group*," *Berkeley Technology Law Journal*, v. 36, n. 1, 2021.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning," arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, "Machine Learning Featurizations for AI Hacking of Political Systems," arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, "Rechanneling Beliefs: How Information Flows Hinder or Help Democracy," Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, "The Coming AI Hackers," Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, "Chinese Technology Platforms Operating in the United States: Assessing the Threat," *Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law*, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, "Legal Risks of Adversarial Machine Learning Research," arXiv:2006.16179.

N. Kim, T. Herr, and B. Schneier, "The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain," *Atlantic Council*, June 2020.

K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships," *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, "Weaponizing Digital Health Intelligence," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, "Politics of Adversarial Machine Learning," *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, "Superheroes on Screen: Real Life Lessons for Security Debates," *Security Journal*, 2019.

H. Farrell, B. Schneier, "Common-Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7, October 2018.

T. Herr, B. Schneier, and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," July 2017 (revised October 2017).

O. S. Kerr, B. Schneier, "Encryption Workarounds," March 2017.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, "Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure'?," *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity,* November 2015.

B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, "Surreptitiously Weakening Cryptographic Systems," *Cryptology ePrint Archive* Report 2015/097, 2015.

104 additional academic publications before August 2014.

Published Articles

"The Hacking of Culture and the Creation of Socio-Technical Debt," *e-flux*, June 18, 2024.

"Using AI for Political Polling," *Harvard Kennedy School Ash Center*, June 11, 2024.

"Indian Election Was Awash in Deepfakes—but AI Was a Net Positive for Democracy," *The Conversation*, June 7, 2024.

"How Online Privacy Is Like Fishing," *IEEE Spectrum*, June 4, 2024.

"How AI Will Change Democracy," *Cyberscoop*, May 28, 2024.

"Seeing Like a Data Structure," *Harvard Kennedy School Belfer Center*, May 25, 2024.

"Lattice-Based Cryptosystems and Quantum Cryptanalysis," *Communications of the ACM*, May 25, 2024.

"LLMs' Data-Control Path Insecurity," *Communications of the ACM*, May 12, 2024.

"AI and Trust," *The Herald Business*, April 30, 2024.

"It's the End of the Web as We Know It," *The Atlantic*, April 24, 2024.

"Backdoor in XZ Utils That Almost Happened," *Lawfare*, April 9, 2024.

"In Memoriam: Ross Anderson, 1956-2024," *Communications of the ACM*, April 9, 2024.

"Public AI as an Alternative to Corporate AI," *New America*, March 14, 2024.

"Let's Not Make the Same Mistakes with AI That We Made with Social Media," *MIT Technology Review*, March 13, 2024.

"How Public AI Can Strengthen Democracy," *Brookings*, March 4, 2024.

"How the 'Frontier' Became the Slogan of Uncontrolled AI," *Jacobin*, February 28, 2024.

"Building a Cyber Insurance Backstop Is Harder Than It Sounds," *Lawfare*, February 26, 2024.

"CFPB's Proposed Data Rules Would Improve Security, Privacy and Competition," *Cyberscoop*, January 26, 2024.

"Don't Talk to People Like They're Chatbots," *Atlantic*, January 17, 2024.

"AI Needs to Be Both Trusted and Trustworthy," *Wired*, January 1, 2024.

"AI Could Improve Your Life by Removing Bottlenecks between What You Want and What You Get," *The Conversation*, December 21, 2023.

"The Internet Enabled Mass Surveillance. AI Will Enable Mass Spying," *Slate*, December 4, 2023.

"AI and Trust," *Harvard Kennedy School Belfer Center*, December 1, 2023.

"Ten Ways AI Will Change Democracy," *Harvard Kennedy School Ash Center*, November 6, 2023.

"Trustworthy AI Means Public AI," *IEEE Security & Privacy*, November 1, 2023.

"Who's Accountable for AI Usage in Digital Campaign Ads? Right Now, No One," *Harvard Kennedy School Ash Center*, October 11, 2023.

"AI Disinformation Is a Threat to Elections—Learning to Spot Russian, Chinese and Iranian Meddling in Other Countries Can Help the Us Prepare for 2024," *The Conversation*, September 29, 2023.

"The A.I. Wars Have Three Factions, and They All Crave Power," *New York Times*, September 28, 2023.

"Robots Are Already Killing People," *Atlantic*, September 6, 2023.

"Nervous About ChatGPT? Try ChatGPT With a Hammer," *Wired*, August 29, 2023.

"Re-Imagining Democracy for the 21st Century, Possibly Without the Trappings of the 18th Century," *The Conversation*, August 7, 2023.

"Six Ways That AI Could Change Politics," *MIT Technology Review*, July 28, 2023.

"Can You Trust AI? Here's Why You Shouldn't," *The Conversation*, July 20, 2023.

"AI Microdirectives Could Soon Be Used for Law Enforcement," *Slate*, July 17, 2023.

"Will AI Hack Our Democracy?," *Harvard Kennedy School Magazine*, July 14, 2023.

"Snowden Ten Years Later," *RFC 9446*, July 1, 2023.

"Artificial Intelligence Can't Work Without Our Data," *Politico*, June 29, 2023.

"AI Could Shore Up Democracy—Here's One Way," *The Conversation*, June 20, 2023.

"Build AI by the People, for the People," *Foreign Policy*, June 12, 2023.

"Big Tech Isn't Prepared for A.I.'s Next Chapter," *Slate*, May 30, 2023.

"Rethinking Democracy for the Age of AI," *Cyberscoop*, May 10, 2023.

"Can We Build Trustworthy AI?," *Gizmodo*, May 4, 2023.

"Just Wait Until Trump Is a Chatbot," *The Atlantic*, April 28, 2023.

"How Artificial Intelligence Can Aid Democracy," *Slate*, April 21, 2023.

"Brace Yourself for a Tidal Wave of ChatGPT Email Scams," *Wired*, April 4, 2023.

"How AI Could Write Our Laws," *MIT Technology Review*, March 14, 2023.

"Why the U.S. Should Not Ban TikTok," *Foreign Policy*, February 23, 2023.

"Everything Is Hackable," *Slate*, February 10, 2023.

"We Don't Need to Reinvent Our Democracy to Save It from AI," *Harvard Kennedy School Belfer Center*, February 9, 2023.

"The Big Idea: Bruce Schneier," *Whatever*, February 7, 2023.

"Opinion: What Peter Thiel and the 'Pudding Guy' revealed," *CNN*, February 7, 2023.

"How ChatGPT Hijacks Democracy," *New York Times*, January 15, 2023.

"How to Decarbonize Crypto," *Atlantic*, December 6, 2022.

"Centralized vs. Decentralized Data Systems—Which Choice Is Best?" *VentureBeat*, September 12, 2022.

"NIST's Post-Quantum Cryptography Standards Competition," *IEEE Security & Privacy*, August 7, 2022.

"When Corporate Interests and International Cyber Agreements Collide," *Cipher Brief*, May 5, 2022.

"Why Vaccine Cards Are So Easily Forged," *The Atlantic*, March 8, 2022.

"Letter to the US Senate Judiciary Committee on App Stores," January 31, 2022.

"Robot Hacking Games," *IEEE Security & Privacy*, January 1, 2022.

"How to Cut Down on Ransomware Attacks Without Banning Bitcoin," *Slate*, June 17, 2021.

"Hacked Drones and Busted Logistics Are the Cyber Future of Warfare," *Brookings TechStream*, June 5, 2021.

"Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy*, May 24, 2021.

"'Grassroots' Bot Campaigns Are Coming. Governments Don't Have a Plan to Stop Them.," *The Washington Post*, May 20, 2021.

"Hackers Used to Be Humans. Soon, AIs Will Hack Humanity," *Wired*, April 19, 2021.

"Bitcoin's Greatest Feature Is Also Its Existential Threat," *Wired*, March 9, 2021.

"Illuminating SolarStorm: Implications for National Strategy and Policy," *Aspen Institute*, March 04, 2021.

"Why Was SolarWinds So Vulnerable to a Hack?" *New York Times*, February 23, 2021.

"The Government Will Guard Biden's Peloton from Hackers. What About the Rest of Us?," *The Washington Post*, February 2, 2021.

"The Solarwinds Hack Is Stunning. Here's What Should Be Done," *CNN*, January 5, 2021.

"Audio: Firewalls Don't Stop Dragons Podcast," *Firewalls Don't Stop Dragons*, December 28, 2020.

"Audio: The Hack by Russia Is Huge. Here's Why It Matters.," *MPR News*, December 28, 2020.

"Review of Data and Goliath (German)," *Nerdhalla*, December 27, 2020.

"Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?," *LA Times*, December 24, 2020.

"Video: AshbrookLIVE #14 – Bruce Schneier," *AshbrookLIVE*, December 24, 2020.

"Audio: Full Disclosure with Bruce Schneier," *BarCode*, December 20, 2020.

"Audio: How Your Digital Footprint Makes You the Product," *TechSequences*, December 16, 2020.

"Video: Hack in the Box Security Conference Keynote Interview," *Hack In The Box Security Conference*, December 3, 2020.

"Video: Election Security: Securing the Vote While Securing the System," *The Legal Edition*, November 19, 2020.

"#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier," *Infosecurity*, November 18, 2020.

"Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair," *Pioneer Institute*, October 13, 2020.

"Audio: We Live in a Security and Privacy World that Science Fiction Didn't Predict," *OWASP PDX Podcast*, October 4, 2020.

"How Amazon and Walmart Could Fix IoT Security," *Data Breach Today*, June 26, 2020.

"The Cyberflâneur #29: Bruce Schneier," *The Syllabus*, June 16, 2020.

"Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series," *Blockchain Rules Podcast*, June 16, 2020.

"Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy," *Policy Punchline*, June 2, 2020.

"Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»," *Open*, June 2, 2020.

"Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World," *Policy Punchline*, May 29, 2020.

"Audio: Bruce Schneier on Truth, Reality, and Contact Tracing," *Reality 2.0*, May 27, 2020.

"Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas," *Cyber Cyber Cyber Cyber*, May 19, 2020.

"The Public Good Requires Private Data," *Foreign Policy*, May 16, 2020.

"How Hackers and Spies Could Sabotage the Coronavirus Fight," *Foreign Policy*, February 28, 2020.

"Technologists vs. Policy Makers," *IEEE Security & Privacy*, January/February 2020.

"We're Banning Facial Recognition. We're Missing the Point.," *The New York Times*, January 20, 2020.

"China Isn't the Only Problem With 5G," *Foreign Policy*, January 10, 2020.

"Bots Are Destroying Political Discourse As We Know It," *The Atlantic*, January 7, 2020.

"We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It," *World Economic Forum*, November 12, 2019.

"Every Part of the Supply Chain Can Be Attacked," *The New York Times*, September 25, 2019.

"The Real Threat from China Isn't 'Spy Trains,'" *CNN*, September 21, 2019.

"What Digital Nerds and Bio Geeks Have to Worry About," *CNN*, September 13, 2019.

"The Myth of Consumer Security," *Lawfare*, August 26, 2019.

"8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, August 12, 2019.

"Attorney General William Barr on Encryption Policy," *Lawfare*, July 23, 2019.

"We Must Prepare for the Next Pandemic," *The New York Times*, June 17, 2019.

"AI Has Made Video Surveillance Automated and Terrifying," *Motherboard*, June 13, 2019.

"AI Can Thrive in Open Societies," *Foreign Policy*, June 13, 2019.

"When Fake News Comes to Academia," *Lawfare*, May 24, 2019.

"Democracy's Dilemma," *Boston Review*, May 15, 2019.

"Russia's Attacks on Our Democratic Systems Call for Diverse Countermeasures," *The Hill*, May 7, 2019.

"Toward an Information Operations Kill Chain," *Lawfare*, April 24, 2019.

"A New Privacy Constitution for Facebook," *OneZero*, March 8, 2019.

"Cybersecurity for the Public Interest," *IEEE Security & Privacy*, January/February 2019.

"There's No Good Reason to Trust Blockchain Technology," *Wired*, February 6, 2019.

"The Public-Interest Technologist Track at the RSA Conference," *RSA Conference Blogs*, January 29, 2019.

"Defending Democratic Mechanisms and Institutions against Information Attacks," *Defusing Disinfo*, January 28, 2019.

"Evaluating the GCHQ Exceptional Access Proposal," *Lawfare*, January 17, 2019.

"Machine Learning Will Transform How We Detect Software Vulnerabilities," *SecurityIntelligence*, December 18, 2018.

"The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia," *Motherboard*, November 19, 2018.

"Surveillance Kills Freedom By Killing Experimentation," *Wired*, November 16, 2018.

"Information Attacks on Democracies," *Lawfare*, November 15, 2018.

"We Need Stronger Cybersecurity Laws for the Internet of Things," *CNN*, November 9, 2018.

"Nobody's Cellphone Is Really That Secure," *The Atlantic*, October 26, 2018.

"Internet Hacking Is About to Get Much Worse," *New York Times*, October 11, 2018.

"Cryptography after the Aliens Land," *IEEE Security & Privacy*, September/October 2018.

"Don't Fear the TSA Cutting Airport Security. Be Glad That They're Talking about It," *Washington Post*, August 17, 2018.

"Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7, 2018.

"Why the FBI Wants You to Reboot Your Router — and Why That Won't Be Enough Next Time," *The Washington Post*, June 6, 2018.

"Data Protection Laws Are Shining a Needed Light on a Secretive Industry," *The Guardian*, June 1, 2018.

"What 'Efail' Tells Us About Email Vulnerabilities and Disclosure," *Lawfare*, May 24, 2018.

"Banning Chinese Phones Won't Fix Security Problems with Our Electronic Supply Chain," *The Washington Post*, May 8, 2018.

"American Elections Are Too Easy to Hack. We Must Take Action Now," *The Guardian*, April 18, 2018.

"It's Not Just Facebook. Thousands of Companies are Spying on You," *CNN*, March 26, 2018.

"Artificial Intelligence and the Attack/Defense Balance," *IEEE Security & Privacy*, March/April 2018.

"Can Consumers' Online Data Be Protected?," *CQ Researcher*, February 9, 2018.

"How to Fight Mass Surveillance Even Though Congress Just Reauthorized It," *The Washington Post*, January 25, 2018.

"The New Way Your Computer Can Be Attacked," *The Atlantic*, January 22, 2018.

"The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse," *CNN*, January 5, 2018.

"How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You," *The Washington Post*, November 27, 2017.

"Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection," , November 1, 2017.

"Don't Waste Your Breath Complaining to Equifax about Data Breach ," *CNN*, September 11, 2017.

"IoT Security: What's Plan B?," *IEEE Security & Privacy*, September/October 2017.

"'Twitter and Tear Gas' Looks at How Protest Is Fueled and Crushed by the Internet," *Motherboard*, July 11, 2017.

"Why the NSA Makes Us More Vulnerable to Cyberattacks," *Foreign Affairs*, May 30, 2017.

"Who Are the Shadow Brokers?," *The Atlantic*, May 23, 2017.

"What Happens When Your Car Gets Hacked?," *The New York Times*, May 19, 2017.

"Why Extending Laptop Ban Makes No Sense," *CNN*, May 16, 2017.

"The Next Ransomware Attack Will Be Worse than WannaCry," *The Washington Post*, May 16, 2017.

"Three Lines of Defense against Ransomware Attacks," *New York Daily News*, May 15, 2017.

"Online Voting Won't Save Democracy," *The Atlantic*, May 10, 2017.

"Who Is Publishing NSA and CIA Secrets, and Why?," *Lawfare*, April 27, 2017.

"The Quick vs the Strong: Commentary on Cory Doctorow's *Walkaway*," *Crooked Timber*, April 26, 2017.

"Infrastructure Vulnerabilities Make Surveillance Easy," *Al Jazeera*, April 11, 2017.

"Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress," *The Guardian*, March 30, 2017.

"Puzzling out TSA's Laptop Travel Ban," *CNN*, March 22, 2017.

"Security Orchestration for an Uncertain World," *SecurityIntelligence*, March 21, 2017.

"How to Keep Your Private Conversations Private for Real," *The Washington Post*, March 8, 2017.

"Botnets of Things," *MIT Technology Review*, March/April 2017.

"Click Here to Kill Everyone," *New York Magazine*, January 27, 2017.

"Why Proving the Source of a Cyberattack is So Damn Difficult," *CNN*, January 5, 2017.

"Class Breaks," *Edge*, December 30, 2016.

"U.S. Elections Are a Mess, Even Though There's No Evidence This One Was Hacked," *The Washington Post*, November 23, 2016.

"Testimony at the U.S. House of Representatives Joint Hearing 'Understanding the Role of Connected Devices in Recent Cyber Attacks,'" November 16, 2016.

"American Elections Will Be Hacked," *The New York Times*, November 9, 2016.

"Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations.," *The Washington Post*, November 3, 2016.

"Lessons From the Dyn DDoS Attack," *SecurityIntelligence*, November 1, 2016.

"Cybersecurity Issues for the Next Administration," *Time*, October 13, 2016.

"We Need to Save the Internet from the Internet of Things," *Motherboard*, October 6, 2016.

"How Long Until Hackers Start Faking Leaked Documents?," *The Atlantic*, September 13, 2016.

"Someone Is Learning How to Take Down the Internet," *Lawfare*, September 13, 2016.

"Stop Trying to Fix the User," *IEEE Security & Privacy*, September/October 2016.

"New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked," *Vox*, August 24, 2016.

"Hackers Are Putting U.S. Election at Risk," *CNN*, July 28, 2016.

"By November, Russian Hackers Could Target Voting Machines," *The Washington Post*, July 27, 2016.

"The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," *Motherboard*, July 25, 2016.

"Credential Stealing as Attack Vector," *Xconomy*, April 20, 2016.

"The Value of Encryption," *The Ripon Forum*, April 2016.

"Can You Trust IRS to Keep Your Tax Data Secure?," *CNN*, April 13, 2016.

"Your iPhone Just Got Less Secure. Blame the FBI.," *The Washington Post*, March 29, 2016.

"Cryptography Is Harder Than It Looks," *IEEE Security & Privacy*, January/February 2016.

"Data Is a Toxic Asset, So Why Not Throw It Out?," *CNN*, March 1, 2016.

"A 'Key' for Encryption, Even for Good Reasons, Weakens Security," *The New York Times Room for Debate*, February 23, 2016.

"Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case," *The Washington Post*, February 18, 2016.

"Candidates Won't Hesitate to Use Manipulative Advertising to Score Votes," *The Guardian*, February 4, 2016.

"The Internet Of Things Will Be The World's Biggest Robot," *Forbes*, February 2, 2016.

"Security vs. Surveillance," *Don't Panic: Making Progress on the 'Going Dark' Debate*, February 1, 2016.

"When Hacking Could Enable Murder," *CNN*, January 26, 2016.

"How an Overreaction to Terrorism Can Hurt Cybersecurity," *MIT Technology Review*, January 25, 2016.

"The Internet of Things That Talk About You Behind Your Back," *Motherboard*, January 8, 2016.

"The Risks—and Benefits—of Letting Algorithms Judge Us," *CNN*, January 6, 2016.

"How the Internet of Things Limits Consumer Choice," *The Atlantic*, December 24, 2015.

"Can Laws Keep Up with Tech World?," *CNN*, December 21, 2015.

"The Automation of Reputation," *Edge.org*, November 5, 2015.

"The Rise of Political Doxing," *Motherboard*, October 28, 2015.

"Face Facts about Internet Security," *CNN*, October 23, 2015.

"The Era Of Automatic Facial Recognition And Surveillance Is Here, *Forbes*, September 29, 2015.

"Stealing Fingerprints," *Motherboard*, September 29, 2015.

"VW Scandal Could Just Be the Beginning," *CNN*, September 28, 2015.

"Living in Code Yellow," *Fusion*, September 22, 2015.

"Hacking Team, Computer Vulnerabilities, and the NSA," *Georgetown Journal of International Affairs*, September 13, 2015.

"Is It OK to Shoot Down a Drone over Your Backyard?" *CNN*, September 9, 2015.

"The Meanest Email You Ever Wrote, Searchable on the Internet," *Atlantic*, September 8, 2015.

"Should Some Secrets Be Exposed?" *CNN*, July 7, 2015.

"Why We Encrypt," Foreword to Privacy International's *Securing Safe Spaces Online*, June 2015.

"China and Russia Almost Definitely Have the Snowden Docs," *Wired,* June 16, 2015

"Why are We Spending $7 Billion on TSA?" *CNN,* June 5, 2015

"Debate: Should Companies Do Most of Their Computing in the Cloud?" *The Economist,* June 5, 2015

"How We Sold Our Souls—and More—to the Internet Giants," *The Guardian,* May 17, 2015

"Could Your Plane Be Hacked?" *CNN,* April 16, 2015

"Baseball's New Metal Detectors Won't Keep You Safe. They'll Just Make You Miss a Few Innings," *The Washington Post,* April 14, 2015

"The Big Idea: *Data and Goliath*," *Whatever*, March 4, 2015.

"Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle," *The Christian Science Monitor*, March 4, 2015.

"The World's Most Sophisticated Hacks: Governments?," *Fortune*, March 3, 2015.

"Cyberweapons Have No Allegiance," *Motherboard*, February 25, 2015.

"Everyone Wants You To Have Security, But Not from Them," *Forbes*, February 23, 2015.

"Your TV May Be Watching You," *CNN*, February 11, 2015.

"When Thinking Machines Break The Law," *Edge*, January 28, 2015.

"The Importance of Deleting Old Stuff—Another Lesson From the Sony Attack," *Ars Technica*, January 12, 2015.

"The Government Must Show Us the Evidence That North Korea Attacked Sony," *Time*, January 5, 2015.

"We Still Don't Know Who Hacked Sony," *The Atlantic*, January 5, 2015.

"2015: The Year 'Doxing' Will Hit Home, *BetaBoston*, December 31, 2014.

"Did North Korea Really Attack Sony?," *The Atlantic*, December 22, 2014.

"Sony Made It Easy, but Any of Us Could Get Hacked," *The Wall Street Journal*, December 19, 2014.

"The Best Thing We Can Do About the Sony Hack Is Calm Down," *Motherboard*, December 19, 2014.

"What Are the Limits of Police Subterfuge?," *The Atlantic*, December 17, 2014.

"Over 700 Million People Taking Steps to Avoid NSA Surveillance," *Lawfare*, December 15, 2014.

"NSA Hacking of Cell Phone Networks," *Lawfare*, December 8, 2014

"Antivirus Companies Should Be More Open About Their Government Malware Discoveries," *MIT Technology Review*, December 5, 2014.

"Why Uber's 'God View' Is Creepy," *CNN*, December 4, 2014.

"Stop the Hysteria over Apple Encryption," *CNN*, October 3, 2014.

"The Future of Incident Response," *IEEE Security & Privacy*, September/October 2014

424 additional published articles before August 2014.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,626,667, January 7, 2014.

77 additional patents before 2014.

Testimonies

Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-04688-RS, United States District Court for the Northern California District. Expert witness for Rodriguez et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2023).

Chasom Brown, William Byatt, Jeremy David, Christopher Castillo, and Monique Trujillo, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-03664-YGR-SVK, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2022).

9 additional depositions before August 2020.